



MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

PROJETO:

EQUARS

EQUARS SPACE SEGMENT DEPENDABILITY PLAN

DOCUMENTO: EQUAR-4920-PLN-001-A		ESTADO: APROVADO
DESCRIÇÃO: Este documento estabelece o plano de Dependabilidade do segmento espacial da Missão EQUARS.		
DATA: 19/09/2019	EDT: 4920 - DEPENDABILIDADE	PÁGINAS: 16



P/

Junat H. L. Bro

ASSINATURA

[Handwritten signature]

[illegible]

SUMÁRIO

1	INTRODUÇÃO.....	7
1.1	ESCOPO DO DOCUMENTO	7
1.2	DOCUMENTOS APLICÁVEIS E DE REFERÊNCIA.....	7
1.2.1	<i>Documentos Aplicáveis (DA)</i>	7
1.2.2	<i>Documentos de Referência (DR)</i>	7
1.3	ACRÔNIMOS E DEFINIÇÕES	7
1.3.1	<i>Lista de Acrônimos</i>	7
1.3.2	<i>Lista de Definições</i>	7
2	GENERAL.....	8
2.1	APPLICABILITY	8
2.2	OBJECTIVES AND BASIC APPROACH	8
3	DEPENDABILITY PROGRAMME MANAGEMENT.....	9
3.1	ORGANIZATION	9
3.2	DEPENDABILITY PROGRAMME PLANNING	9
3.3	DEPENDABILITY CRITICAL ITEMS.....	9
3.4	DESIGN REVIEWS.....	10
3.5	DOCUMENTATION (TBD).....	10
4	DEPENDABILITY ENGINEERING (TBD)	11
4.1	INTEGRATION OF DEPENDABILITY IN THE PROJECT (TBD)	11
4.2	DEPENDABILITY REQUIREMENTS IN TECHNICAL SPECIFICATIONS (TBD)	11
4.3	DEPENDABILITY DESIGN CRITERIA (TBD).....	11
4.4	INVOLVEMENT IN TESTING PROCESS (TBD)	11
4.5	INVOLVEMENT IN OPERATIONAL ASPECTS (TBD)	11
5	DEPENDABILITY ANALYSES.....	12
5.1	RELIABILITY ANALYSIS (TBC).....	12
5.1.1	<i>Reliability Prediction</i>	12
5.1.2	<i>Reliability Block Diagram (Functional Analysis)</i>	12
5.2	PARTS STRESS ANALYSIS (PSA)	13
5.3	FAILURE MODES AND EFFECTS ANALYSES (FMEA)	13
5.4	CRITICAL ITEM LIST (CIL)	14
5.5	AVAILABILITY ANALYSES (TBC).....	15
5.6	MAINTAINABILITY ANALYSES (TBC)	15
	ANEXO A	15
	APÊNDICE A.....	15

LISTA DE FIGURAS

Figura 1	Satellite Dependability Assurance Organization interfaces.	9
----------	---	---

LISTA DE TABELAS

Tabela 1	Satellite Dependability deliverable documents per project review. (TBC)	10
----------	---	----



EM BRANCO



1 INTRODUÇÃO

1.1 ESCOPO DO DOCUMENTO

Este documento estabelece o plano de Dependabilidade do segmento espacial da Missão EQUARS apresentando a organização responsável pelo desenvolvimento e o programa de Dependabilidade.

1.2 DOCUMENTOS APLICÁVEIS E DE REFERÊNCIA

1.2.1 Documentos Aplicáveis (DA)

- [DA-1] EQUARS-3100-TS-001-A – Product Assurance Requirements – Space Segment
- [DA-2] 951/2017/SEI-INPE – Memorando nº 951/2017/SEI-INPE do Processo SEI nº 01340.000977/2017-95.
- [DA-3] EQUARS-3100-PLN-001-A – Product Assurance Plan

1.2.2 Documentos de Referência (DR)

- [DR-1] EQUARS-1140-PLN-001-A - Plano de Gerenciamento de Riscos
- [DR-2] SESEQ-Q-HBK-00047 – Guia de Elaboração das Análises de Confiabilidade (Predição de Confiabilidade, Redução de Esforços (Derating)) e FMEA/FMECA de Partes Elétricas, Eletrônicas e Eletromecânicas para os Satélites do INPE

1.3 ACRÔNIMOS E DEFINIÇÕES

1.3.1 Lista de Acrônimos

- TBC** To Be Confirmed.
- TBD** To Be Defined.

1.3.2 Lista de Definições



2 GENERAL

This Dependability plan establishes the provisions for planning the EQUARS Satellite Dependability efforts. It has been derived from EQUARS Dependability Requirements presented at document [DA-1]. The Dependability programme ensures, through analysis, modelling, testing and reporting, that the customer specifications for high operational Reliability and Availability are met for the overall program success.

2.1 APPLICABILITY

The Space Segment Dependability plan is applicable to INPE Engineering Division (ETE), according to the established work allocation [DA-2], responsible for the design up to SRR of the EQUARS mission development. Otherwise the planning content shall cover all requirements to be fulfilled in the development and implementation phases of the project. The plan fully applies for the design, development, procurement, manufacturing, integration tests and delivery of the following:

- Flight Hardware and flight spare models;
- Hardware subjected to, or participating in, the design verification or qualification testing (TBC);
- Deliverable Ground Support Equipment (GSE) and for GSE items with direct interface to flight hardware (TBC);
- Components procurement for the Satellite (TBC).

2.2 OBJECTIVES AND BASIC APPROACH

The purpose of the Dependability plan is to provide information on the organizational aspects and the technical approach to the execution of the Dependability programme and to describe how the relevant disciplines and activities are coordinated and integrated to fully comply with the requirements. This plan identifies and ties together all the tasks including planning, predictions, analyses, demonstration and defines the methods and the techniques to accomplish the dependability requirements. The plan identifies the prime responsible for the dependability programme. It also includes details of the applicable phases, products and associated hardware relevant to the programme, and describes how dependability is managed throughout the project phases. The Dependability activities include:

- Defining Dependability requirements for all satellite equipment Sub-Contractors/Suppliers.
- Ensuring that all dependability requirements are included in the design in an effective manner.
- Checking that all the suppliers dependability activities are conducted in accordance with the EQUARS programme milestones.
- Providing the dependability data necessary to demonstrate that all the dependability requirements are met.

3 DEPENDABILITY PROGRAMME MANAGEMENT

3.1 ORGANIZATION

EQUARS Dependability Assurance programme is based on EQUARS organization and directly interfaces with the Product Assurance organization. The EQUARS Satellite Dependability Assurance Organization will be responsible for implementing the EQUARS Satellite Dependability Assurance programme. It will define, allocate, disseminate, modify and incorporate the Dependability needs into the mission performances requirements. Figure 1 shows the Satellite Dependability Assurance Organization interfaces and information/communication flow.

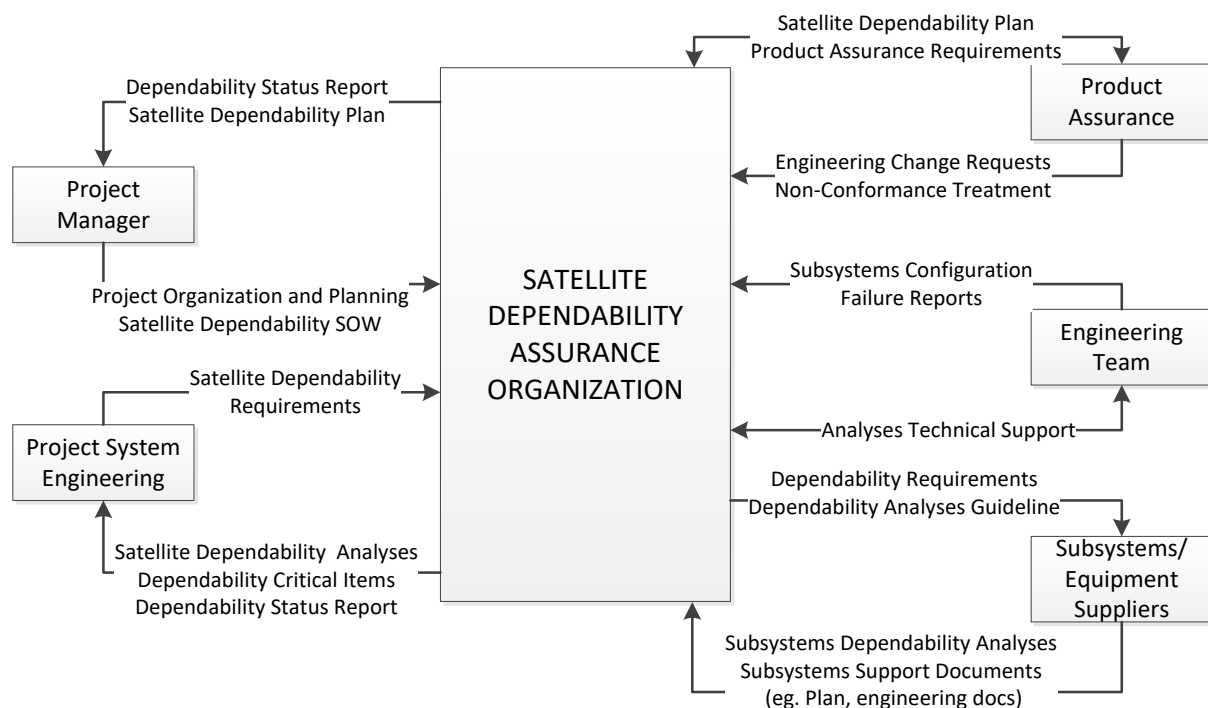


Figura 1 Satellite Dependability Assurance Organization interfaces.

3.2 DEPENDABILITY PROGRAMME PLANNING

The programme describes all the tasks to be conducted and the rationale to achieve the reliability required for the satellite level. This plan will be implemented to find the most reliable design configurations under the given program constraints and to check that dependability design attributes are not degraded by manufacture, assembly, integration, test and operations.

3.3 DEPENDABILITY CRITICAL ITEMS

In line (TBC) with the overall Product Assurance Plan [DA-3] established for Critical Items, the EQUARS Satellite Dependability Assurance Organization will continually assess the dependability risks

and support the processes for their control and mitigation. Dependability will also feed the EQUARS Satellite Risk List by selecting among the Dependability critical items those requiring additional management attention. The risk related activities are according the Risk Management Plan [DR-1].

3.4 DESIGN REVIEWS


Dependability issues will be addressed in each design review. Dependability Analyses will be initiated in the Phase B (TBC) in accordance with [DA-1] and these will be revised as the design matures.

3.5 DOCUMENTATION (TBD)

A Dependability data file will be established; it will contain all technical trade-offs, assessments, analyses related to Dependability and the Dependability recommendations status log. The Satellite Dependability deliverable documents per project review are planned according Table 1.

Tabela 1 Satellite Dependability deliverable documents per project review. (TBC)

Satellite Dependability Documents	Satellite Project Phasing			
	Phase A	Phase B	Phase C	Phase D
Satellite dependability Assurance plan				
Satellite reliability Budget				
Satellite dependability Analyses Report				
Satellite dependability Assurance Requirements Status				
Equipment Dependability Requirements				
Satellite dependability (PDR Data Package)				
Satellite dependability (CDR Data Package)				
Satellite dependability (AR Data Package)				

EQUARS	<p style="text-align: center;">EQUAR-4920-PLN-001-A EQUARS SPACE SEGMENT DEPENDABILITY PLAN</p>	
--------	---	--

4 DEPENDABILITY ENGINEERING (TBD)

4.1 INTEGRATION OF DEPENDABILITY IN THE PROJECT (TBD)

4.2 DEPENDABILITY REQUIREMENTS IN TECHNICAL SPECIFICATIONS (TBD)

4.3 DEPENDABILITY DESIGN CRITERIA (TBD)

4.4 INVOLVEMENT IN TESTING PROCESS (TBD)

4.5 INVOLVEMENT IN OPERATIONAL ASPECTS (TBD)



5 DEPENDABILITY ANALYSES

5.1 RELIABILITY ANALYSIS (TBC)

The reliability analyses realization will be performed according [DR-2].

5.1.1 Reliability Prediction

Applications:

The reliability prediction will be performed at equipment, subsystem and satellite level, and will consider all components of the equipment. The reliability prediction is a bottom-up method where the immediate lower level prediction is input to higher level.

Purpose:

- to predict the in-service reliability of a product;
- to provide failure probability data.

Description of the activity:

The Reliability Prediction will be performed for worst case operating and environmental conditions. The satellite reliability prediction is performed with input from subsystem and equipment analyses.

Outputs:

Satellite Reliability Prediction Analysis

5.1.2 Reliability Block Diagram (Functional Analysis)

Applications:

The Reliability Block Diagram will be performed at equipment, subsystem and satellite level as a basis of all other design activities.

Purpose:

- To determine the basic functions (main and constraint) of the Satellite
- To support reliability modelling and FMEA

Description of the activity:

The list of all the basic functions of the System will be established and their performances will be addressed. Once the design architecture is defined, the functions are apportioned in terms of hardware blocks and software modules.

Outputs:

- List of the main functions at satellite level
- List of the constraint functions at satellite level

- Reliability Block Diagram (Functional Tree) whit part of the Reliability Prediction Analysis and FMEA report.

5.2 PARTS STRESS ANALYSIS (PSA)

Applications:

Derating is an engineering practice carried out on all electrical/electronic parts to ensure that parts are used within the limits of their design. A part stress analysis (PSA) will be performed at unity/equipment level to verify that derating factors with respect to applicable parameters (power, voltage, temperature...) are met under worst-case conditions.

Purpose:

To demonstrate that each EEE part works with an adequate margin, (derating), with respect to the maximum allowable limits specified in the component specification, (rated stresses), in order to improve its failure rate and lifetime.

Description of the activity:

All EEE parts shall respect derating rules specified in ECSS-Q-ST-30-11-C rev 1 document. The PSA will be performed according [DR-2]. The PSA is performed at components/parts level therefore Satellite Dependability Organization is responsible to follow the results and requirements compliance status.

Outputs:

Part Stress Analysis Compliance Status

5.3 FAILURE MODES AND EFFECTS ANALYSES (FMEA)

Applications:

A FMEA will be performed at equipment, subsystem and satellite level by each responsible organization. The FMEA performed at Satellite level will be based on detailed existing FMEA performed at subsystem level for all categories of items excluding pure structure (TBC). The FMEA is a top-down (early phases) and bottom-up method where the immediate lower level prediction is input to higher level and vice-versa. The FMEA will consider the following, minimum number of, failure modes:

- Premature operation;
- Failure to operate at a prescribed time;
- Failure to stop operation at a prescribed time;
- Failure during operation;
- Degradation or out-of-tolerance operation;
- For EEE parts: short circuit, open circuit, incorrect function (such as SEU, latch-up) (TBC)
- Incorrect commands or command sequence;

Purpose:

- To design a failure tolerant architecture (functional FMEA);
- To support failure propagation avoidance;
- To support design team for a reliable architecture design;
- To support telemetry parameters definition and monitoring;
- To support corrective actions (on-board, from ground) definition;
- To identify single point failures;
- To demonstrate failure tolerance requirements are met;
- To support contingency analysis.

Description of the activity:

Early in the design phase, a functional FMEA will be performed at Satellite level based on functional analysis and the preliminary architecture. From this analysis a first set of technical requirements and hazardous events is derived and integrated into the relevant technical specifications. Subsystem FMEA's will be performed at PDR (TBC) and CDR (TBC) and integrated after validation, (design reviews), into the System FMEA. This continuous and iterative process will be finalized by a formal review (Satellite CDR) (TBC). The FMEA analyses realization will be performed according [DR-2].

Outputs:

Satellite Functional FMEA

Input to CIL

Satellite Detailed FMEA

5.4 CRITICAL ITEM LIST (CIL)

Applications:


Product Assurance will establish a Critical Items List (TBC) for Managerial focus and allocation of resources.

Purpose:

The purpose of the Dependability inputs to the CIL is:

- to identify all Dependability critical items (SPF; all items that have failure consequence classified as catastrophic; products that cannot be checked and tested after integration, limited-life products, products that do not meet, or cannot be verified as meeting items; that not meet part stress requirements; items with high predicated failure rates, critical performance or critical function; items that do not meet parts stress requirements.
- to provide a tool for risk management, i.e. either through corrective actions plan in order to eliminate the related items, or through rationale for retention.

Description of the activity:

EQUARS	<p style="text-align: center;">EQUAR-4920-PLN-001-A EQUARS SPACE SEGMENT DEPENDABILITY PLAN</p>	
--------	---	--

All critical items identified through the various Dependability analyses will be incorporated into the CIL and subject to management and control. Each Critical Item that is retained will be supported with a justification for retention and approved (**TBD**). Dependability critical items requiring high-level management and control because of the important risk they exhibit for EQUARS programme will be transferred to the Management Risk list.

Outputs:

Inputs to Critical Item list

Inputs to Risk List

5.5 AVAILABILITY ANALYSES (**TBC**)

5.6 Maintainability Analyses (**TBC**)

LISTA DE ITENS <i>TO BE DEFINED</i>			
ID	DESCRIÇÃO	STATUS	PREVISÃO DE CONCLUSÃO
TBD-1			
LISTA DE ITENS <i>TO BE CONFIRMED</i>			
ID	DESCRIÇÃO	STATUS	PREVISÃO DE CONCLUSÃO
TBC-1	aa		