esa

DOCUMENT

document title/ titre du document

PROBA3 Product Assurance Requirements

prepared by/*préparé par* Ralf Reutemann

reference/*réference* P3-EST-RS-1005
issue/*édition* 1
revision/*révision* 1
date of issue/*date d'édition* 26.08.2008
status/*état* For approval
Document type/*type de document* RQ
Distribution/*distribution*

APPROVAL

Title *Titre*	PROBA3 Product Assurance Requirements	issue *issue* 1	revision *revision* 1
author *auteur*	Ralf Reutemann	date *date*	26.08.2008
approved by *approuvé par*		date *date*	

CHANGE LOG

reason for change */raison du changement*	issue/*issue*	revision/*revision*	date/*date*
Initial version of the document for internal review.	0.1.6	0	26.05.2008
- Update of draft issue in order to reflect up-issued and modified references to ECSS standards - Minor correction of contents - Update of document structure according to standard Template.	1	0	24.07.2008
Issue for preTEB. Removed section references to some ECSS standards.	1	1	26.08.2008

CHANGE RECORD

Issue: 1 Revision: 1

reason for change/*raison du changement*	page(s)/*page(s)*	paragraph(s)/*paragraph(s)*

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 Scope of Document 1
1.2 Definitions 1
1.3 Abbreviations 1

2 APPLICABLE AND REFERENCE DOCUMENTS 2
2.1 Applicable Documents 2
2.2 Applicable Standards and Regulations 2
2.3 Reference Documents 3

3 GENERAL PA REQUIREMENTS 3
3.1 PA Responsibilities 3
3.2 Product Assurance and Safety Plan 4
3.3 PA Objectives 4
3.4 PA Policy 4
3.5 Critical Items (CI) 4
3.6 PA Progress Reporting 5
3.7 Tailoring of PA Requirements 5

4 QUALITY ASSURANCE 6
4.1 QA Approach 6
4.2 Audits 6
4.3 Personnel Training and Certification 6
4.4 Documents and Data Control 7
4.5 Quality Records 7
4.6 Traceability 7
4.7 Metrology and Calibration 7
4.8 Non-Conformance Control System 7
4.9 Waivers/ Deviations 7
4.10 Design and Verification 7
4.11 Design Changes 8
4.12 Procurement Documents 8
4.13 Control of Processes 8
4.14 Cleanliness and Contamination Control 8
4.15 Handling, Storage, Preservation, Marking, Labelling, Packaging and Shipping Control 8
4.16 Failures and Accidents 8
4.17 Receiving Inspection 8
4.18 In-Process Inspection 9
4.19 Workmanship Standards 9

4.20 Temporary Installations and Removals....9
4.21 Logbook....9
4.22 Test Plans....9
4.23 Test Procedures....9
4.24 Test Reports....10
4.25 Test Performance Monitoring....10
4.26 Test Reviews....10
4.27 Acceptance and Delivery....10
4.28 End Item Data Package (EIDP)....11

5 DEPENDABILITY ASSURANCE....11
5.1 Dependability Approach....11
5.2 Dependability Requirements in Technical Specifications....11
5.3 Consequence Severity Categories....12
5.4 Failure Tolerance....12
5.5 Failure Propagation....12
5.6 Dependability Analyses....12
5.7 Single-Point Failure (SPF)....13
5.8 Maintainability....13

6 SAFETY....13
6.1 Safety Approach....13
6.2 Safety Reviews and Meetings....14
6.3 Safety Analyses....14
6.4 Safety Design Principles....14
6.5 Safety Inhibits....14
6.6 Safe Without Services....14
6.7 Design for Minimum Risk....15
6.8 Fracture Control....15
6.9 Safety Factors....15
6.10 Materials....15
6.11 Hazard Tracking....15

7 EEE COMPONENTS....15
7.1 General....15
7.2 Programme Plan....16
7.3 Component Selection....16
7.4 Components Screening....16
7.5 Components Approval....16
7.6 Components Listing....16
7.7 Radiation Tolerance....16
7.8 Programmable Devices....17
7.9 Off-The-Shelf Equipment....17

8 MATERIALS, MECHANICAL PARTS AND PROCESSES....17
8.1 General....17
8.2 Material Approval....17
8.3 Materials, Mechanical Parts and Processes Listing....17
8.4 Materials and Mechanical Parts Requirements....17
8.5 Processes Requirements....18

9 CONFIGURATION MANAGEMENT....18

10 SOFTWARE PRODUCT ASSURANCE....19

11 OFF-THE-SHELF (OTS) EQUIPMENT....19

1 INTRODUCTION

1.1 Scope of Document

This document defines the product assurance requirements application to the PROBA3 project. The satellite shall be designed, manufactured and tested in compliance with these requirements. The requirements are applicable to the supplier (prime and sub-contractors). It is the responsibility of the prime contractor to tailor these requirements, if necessary, to sub-contractors to ensure their implementation.

1.2 Definitions

There are none.

1.3 Abbreviations

AIT	Assembly, Integration and Testing
ASIC	Application Specific Integrated Circuits
CAM	Commercial, Aviation or Military
CI	Critical Item
CIDL	Configuration-Item Data List
CIL	Critical Items List
CM	Configuration Management
DA	Derating Analysis
DCL	Declared Components List
DML	Declared Materials List
DMPL	Declared Mechanical Parts List
DPL	Declared Process List
DRB	Delivery Review Board
EEE	Electronic, Electrical and Electro-mechanical
EDAC	Error Detection And Correction
EPPL	European Preferred Parts List
ESA	European Space Agency
FMEA	Failure Modes Effects Analysis
FPGA	Field Programmable Gate Array
HA	Hazard Analysis
HSIA	Hardware/Software Interaction Analysis
ICD	Interface Control Document
KIP	Key Inspection Point
MIP	Mandatory Inspection Point
NCTS	Non-Conformance Tracking System
NDI	Non-Destructive Inspection

OTS	Off-The-Shelf
PA	Product Assurance
PAD	Part Approval Document
PA&S	Product Assurance and Safety
PCB	Printed-Circuit Board
PTR	Post-Test Review
QA	Quality Assurance
QDR	
RFA	Request for Approval
RFD	Request for Deviation
RFW	Request for Waver
SCC	Stress Corrosion Cracking
SDR	
SPF	Single-Point Failure
SEL	
SEU	Single-Event Upset
TRB	Test Review Board
TRL	Technology Readiness Level
TRR	Test Readiness Review
UV	Ultra-violet
WCA	Worst-Case Analysis

2 APPLICABLE AND REFERENCE DOCUMENTS

2.1 Applicable Documents

The following documents shall be applicable:

AD-1	TEC-Q/08-6889	PA & Safe ty Strategy for In-Orbit Demonstration LightSat Concept

2.2 Applicable Standards and Regulations

SD-1	ECSS-Q-ST-20C	Quality Assurance
SD-2	ECSS-Q-ST-40C	Safety
SD-3	ECSS-Q-ST-60C	EEE Components
SD-4	ECSS-Q-ST-30-11C	Derating - EEE components
SD-5	ECSS-Q-ST-60-02C	ASIC and FPGA development
SD-6	ECSS-E-ST-32-01C	Fracture Control
SD-7	PSS-01-608	Generic specification for hybrid micro-circuits
SD-8	PSS-01-700	The technical reporting and procedures for materials and processes
SD-9	ECSS-Q-ST-70-02C	Thermal vacuum outgassing test for the screening of space materials

SD-10	ECSS-Q-ST-70-08C	The Manual Soldering of High-Reliability Electrical Connections
SD-11	ECSS-Q-ST-70-26C	Crimping of high reliability electrical connections
SD-12	ECSS-Q-ST-70-28C	Repair and modification of printed circuit boards for space use
SD-13	ECSS-Q-ST-70-36C	Material selection for controlling stress corrosion cracking
SD-14	ECSS-Q-ST-70-37C	Determination of the susceptibility of metals to stress corrosion cracking
SD-15	PSS-01-738	High-reliability soldering for surface-mount and mixed-technology printed circuit boards
SD-16		Deleted
SD-17	ECSS-Q-ST-30C	Dependability
SD-18	ECSS-Q-ST-70 C	Materials, Mechanical Parts and Processes
SD-19	ECSS-Q-ST-80C	Software Product Assurance
SD-20	ECSS-M-ST-40C	Configuration and information management
SD-21	ECSS-Q-70-01A	Cleanliness and contamination control
SD-22	PSS-01-202	Preservation, storage, handling and transportation of ESA spacecraft hardware
SD-23	ECSS-Q-ST-30-02C	Failure Modes, Effects (and Criticality) Analysis (FMEA/FMECA)
SD-24	ECSS-Q-ST-40-02C	Hazard analysis
SD-25	ECSS-Q-60-01A	European Preferred Parts List (EPPL) and its management
SD-26	PSS-01-701	Data for the selection of space materials
SD-27	PSS-01-706	The particle and ultraviolet (UV) radiation testing of space materials
SD-28		Deleted
SD-29	ECSS-E-ST-10-03C	Testing
SD-30	ECSS-Q-ST-10C	Product assurance management

2.3 Reference Documents

There are none.

3 GENERAL PA REQUIREMENTS

3.1 PA Responsibilities

The supplier shall identify the personnel responsible for managing and performing the PA activities.

3.2 Product Assurance and Safety Plan

The supplier shall prepare a Product Assurance and Safety Plan (PA&S Plan) that shall cover the following disciplines:

- PA management
- Quality assurance
- Reliability assurance
- Safety
- EEE components
- Materials, mechanical parts and processes
- Configuration management
- Software Product Assurance

These disciplines shall be coordinated as an integrated effort and in cooperation with the functions of project management and engineering.
The PA&S Plan shall describe in detail the resources, tasks, responsibilities, methods and procedures necessary for the implementation of the PA requirements defined in this document and for the achievement of the PA objectives.
The supplier's internal procedures may be referenced in the PA&S Plan. In this case they shall be provided on request. The suppliers should be aware that referencing internal supplier procedures in the PA&S Plan will limit the supplier's ability to unilaterally change the procedures. All modifications to these procedures shall be considered as modification to the PA&S Plan.
The PA&S Plan shall be submitted to the Customer for approval. It shall be implemented and maintained by the supplier throughout the PROBA3 life cycle, and shall be a binding and formal document.

3.3 PA Objectives

The prime objective of the supplier's PA program shall be to assure that the PROBA3 spacecrafts will accomplish the intended mission objectives successfully. This shall be achieved in the most cost-effective way by managing the available resources and personnel within the allocated budget.

3.4 PA Policy

A preventive approach shall be adopted for the early identification of potential problems. Constant interaction with engineering during the development process is required. Verification and certification activities shall be performed to achieve the Customer's final acceptance of the end product. The requirements of SD-30 shall be applicable.

3.5 Critical Items (CI)

The supplier shall identify those items that are critical to safety and reliability (that is, items associated to hazards with catastrophic and critical consequences, see section 5.3) by performing hazard and dependability analyses (such as hazard analysis and FMEA). Specific actions to reduce

the criticality shall be defined and implemented for each critical item. Critical Items (CI) shall be controlled and tracked until final acceptance of flight hardware and software.
Fracture-critical items and single-failure points shall be critical items. The supplier shall draw up a Critical Items List (CIL), which shows the reason for criticality, and the detection and remedy features. The requirements of SD-1 shall be applicable.

3.6 PA Progress Reporting

PA progress reporting shall be part of the overall project progress reporting and shall address:

- Status of the PA activities since the last progress report
- Potential problem areas
- Action items status
- Critical items status
- Non-conformance and waiver status
- Parts, materials and processes qualification status.
- Audit plan status
- Alert status
- PA documentation

3.7 Tailoring of PA Requirements

The PA requirements in this document and the applicable documents in section 2 may be tailored in line with the strategy in AD-1, in combination with the mission success criteria and risk policy in PROBA3, and with ESA approval.
AD-1 presents an alternative option for suppliers. AD-1 outlines ESA's strategy for the adapting PA&S processes to design, development and implementation and to operations, that is targeted at missions in the domain of experiments in space, including technological/small missions. The primary objective is to enable fast development of technology by reducing the program cost and schedule while maintaining acceptable levels of quality/ risk for this particular class of missions. The main concepts guiding the adaptation of PA&S processes focus on identifying and supporting opportunities to reduce workload associated to PA&S processes by introducing/exploiting:

- New techniques, methods, tools
- Extensive use of tools between users-ESA-industry, warranting continuous visibility to all team members
- Different required levels of reliability as part of risk policy: Platform-robust "safe mode"/payload-technology demonstrators
- New approach to project reviews, making efficient use of common, comprehensive development environment

Following the lead in bullet three above, it is recommended to structure the PA&S strategy in four classes:

- **Safe Mode:** Spacecraft components or functions that are necessary to ensure the survival of the spacecraft. For example, Sun-pointing algorithms and sensors triggered in case of general malfunction
- **Platform:** Spacecraft element that carries the payload and provides housekeeping functions
- **Technology:** Spacecraft components or functions whose Technology Readiness Level (TRL) is to be increased as part of the mission objectives. This could be a technology at TRL 5 ("component and/or breadboard validation in relevant environment"), for example a new type of reaction wheel, that is aimed to be raised to increase to TRL 6 ("system/subsystem model or prototype demonstration in a relevant environment --- ground or space") or 7 ("system prototype demonstration in a space environment")
- **Other:** Any other spacecraft component or function that does not fall under any of the previous classes

In summary, the idea is to first pay special attention to cost/schedule optimization opportunities generated by working differently and by the introduction of effective tools and integrated teams, and second focus on relaxation of requirements in line with risk policy (see AD-1), and third, structure the strategy into the four classes: Safe Mode, Platform, Technology and Other.

4 QUALITY ASSURANCE

4.1 QA Approach

The supplier shall establish and implement a QA program for all mission phases. The requirements of SD-1 shall be applicable, with the possibility for tailoring by the prime as described in section 3.7.

4.2 Audits

The supplier shall establish and maintain an Audit plan (annex to the PA&S plan) covering external and in-house audits to verify the implementation and effectiveness of the PA program.
The Audit plan shall be subject to the Customer's approval.
The Customer shall have the right to be represented in all audits.
The Customer shall have the right to audit any supplier at any time.
In addition to the planned audits, special audits may be performed in case of failure, poor quality or other problems.
A copy of the audit report shall be sent to the Customer within 2 weeks after the audit.

4.3 Personnel Training and Certification

The supplier shall establish a documented training program according to SD-1 for all personnel whose performance determines or affects product quality, such as those operators performing critical processes.

4.4 Documents and Data Control

The supplier shall control documentation and data according to SD-1 section 5.1 (Documentation and data control).

4.5 Quality Records

The supplier shall maintain quality records to provide objective evidence of complete and effective performance of QA activities and to demonstrate the achievement of the required quality.
Quality records shall be stored in a way to prevent alteration, loss or deterioration, for at least ten year after the end of mission.

4.6 Traceability

The supplier shall implement a traceability system according to AD-1 section 5.4.

4.7 Metrology and Calibration

All measuring, inspection and test equipment used during verification activities shall be controlled and calibrated on a regular basis according to the requirements of SD-1. Calibration records shall be maintained.

4.8 Non-Conformance Control System

The supplier shall establish and maintain a non-conformance control system according to the requirements of SD-1. The use of NCTS (Non-Conformance Tracking System) shall be considered and in case the use of another system is proposed, it shall be justified and submitted to the Customer for approval
The supplier PA shall notify all major non-conformances to the Customer within 1 day. The supplier PA shall notify all minor non-conformances to the Customer within 1 week.

4.9 Waivers/ Deviations

The supplier shall submit a Request for Waver (RFW) / Request for Deviation (RFD) to the Customer for approval in order to formalize the difference with the required baseline, or when a requirement cannot be met.

4.10 Design and Verification

The supplier shall perform design and verification according to SD-1 sections 6.4 (Design rules) and 6.6 (Verification).

4.11 Design Changes

The supplier shall implement a QA program to assure that all design changes and modifications are identified, documented, classified, reviewed and approved before their implementation.

4.12 Procurement Documents

The supplier shall ensure that procurement documentation complies with the requirements in SD-1 section 7.3 (Procurement documents).

4.13 Control of Processes

The supplier shall ensure during manufacturing, assembly and integration that processes are controlled according to SD-1 section 8.4 (Control of processes).

4.14 Cleanliness and Contamination Control

The supplier shall establish requirements and controls for molecular and particulate cleanliness of flight hardware and facilities. The requirements in SD-21 shall be applicable.
The controls to be applied shall be specified in a Cleanliness and Contamination Control plan (annex of the PA&S plan).
The supplier shall evaluate the sensitivity to contamination of the hardware and define the corresponding cleanliness levels to be applied during all phases of manufacture, assembly, integration and test.
The required cleanliness levels shall be specified in design drawings, specifications and procedures.

4.15 Handling, Storage, Preservation, Marking, Labelling, Packaging and Shipping Control

The supplier shall establish requirements and procedures for handling, storage, preservation, marking, labelling, packaging and shipping. The requirements in SD-22 shall be applicable.

4.16 Failures and Accidents

Failure and accidents shall be processed according to the non-conformance control system, and treated as a major non-conformance

4.17 Receiving Inspection

All incoming supplies (including documentation) shall be inspected by the supplier to verify conformance with the requirements of the procurement documents.
Inspections shall be performed according to established procedures and instructions.

4.18 In-Process Inspection

The supplier shall perform inspections during manufacturing, assembly and integration in accordance with SD-1 section 8.9 (Inspection).
The supplier shall identify Mandatory Inspection Points (MIPs) prior to SDR. The supplier shall deliver a MIP plan at the SDR for Customer approval.

4.19 Workmanship Standards

The supplier shall employ workmanship standards during manufacturing, testing and integration, to ensure acceptable and consistent workmanship quality levels.

4.20 Temporary Installations and Removals

The supplier shall control flight items that are temporarily removed or non-flight items that are temporarily installed according to the requirements of SD-1 section 8.10.1 (Control of temporary installations and removals).

4.21 Logbook

The supplier shall prepare and maintain logbooks for all operations and tests performed on PROBA3 hardware according to the requirements of SD-1. Logbooks shall comply with the requirements of SD-1 section 8.10.2 (Logbooks).

4.22 Test Plans

Tests shall be performed according to test plans approved by the Customer. Test plans shall be written in accordance with SD-29 and shall show how compliance with requirements is intended to be demonstrated, and shall highlight any special equipment or facility that is necessary to conduct the tests.

4.23 Test Procedures

Tests shall be performed according to documented test procedures. These shall include:

- Scope of the test
- Identification of the test article
- Applicable documents
- Test flow
- Test organization
- Test conditions
- Test equipment and set up
- Step-by-step procedure
- Pass/ fail criteria and test requirements

Test procedures require the Customer approval

4.24 Test Reports

The supplier shall prepare reports in accordance with SD-29 to document the tests performed.

4.25 Test Performance Monitoring

The supplier shall define how test activities are monitored, how test procedures are followed and how any deviation is reported and treated, according to the requirements of SD-1 section 9.4 (Test performance monitoring).

4.26 Test Reviews

Test reviews shall be performed before and after major test activities of the qualification and acceptance program (e.g., vibration test).

The purpose of the Test Readiness Review (TRR) shall be to:
- Assess the as-built status of the items to be tested against the required configuration;
- Review the status of non-conformances to verify that those still open have no impact on the validity of the test;
- Review approval status of the test procedure;
- Assess the readiness of the test facility (including safety aspects).

The purpose of the Post-Test Review (PTR) shall be to:
- Verify the completeness of the test data and their conformance to the requirements. If the test was successful, state that test results comply with the requirements and the test item can be processed/ tested further;
- Verify that all deviations from the initial test procedure were authorized;
- Verify that non-conformance and failures during the test were recorded and disposed.

Reviews shall be conducted by a Test Review Board (TRB) consisting of at least:
- The PA representative (chairman);
- The engineering representative;
- The AIT representative;
- Customer representative(s), unless specifically waived by the Customer.

4.27 Acceptance and Delivery

The supplier shall establish a formal acceptance process for all configuration items to ensure that conformance of the items to be delivered is fully assessed and documented.
The supplier shall ensure that a Delivery Review Board (DRB) is convened prior to the delivery, according to the requirements of SD-1 section 10.3 (Delivery review board).

4.28 End Item Data Package (EIDP)

The supplier shall prepare an EIDP for each deliverable end item.

The EIDP shall contain, as a minimum:

- Certificate of conformance
- As-built configuration list
- Critical items list
- Limited life items list
- Temporary installation records
- Open/ deferred work, open tests
- Qualification status list
- Non-conformance list
- Deviations and waivers list
- Cleanliness certificate
- Safety assessment
- Verification control document
- Loose delivered items list
- Operation and maintenance manual
- Special packaging and shipping procedure
- CIDL
- DRB minutes
- MIP & KIP reports
- Log book
- ICD

The content of the EIDP shall be finalized at the QDR.

5 DEPENDABILITY ASSURANCE

5.1 Dependability Approach

The supplier shall develop and implement design criteria and dependability requirements to ensure that reliability is built into the design through the use of failure tolerance and design margins. The supplier shall perform dependability analyses to support the design and qualification process, and to show compliance with the dependability requirements.
The requirements of SD-17 shall be applicable, with the possibility for tailoring by the prime as described in section 3.7.

5.2 Dependability Requirements in Technical Specifications

The supplier shall include dependability requirements during the preparation and review of design and test specifications. To this purpose, the following shall be included in the specifications:

- Functional, operational and environmental requirements
- Test requirements
- Design margins, derating factors
- Failure tolerance
- Fault detection and recovery of the system and its restoration to an acceptable state
- Failure propagation across interfaces among subsystems and with the carrier

5.3 Consequence Severity Categories

Failures or hazardous events shall be classified according to their consequences, according to AD-1 section 5.2.1.2 “Consequence Category and Severity.”
All failure scenarios identified through dependability analyses (see section 5.6) shall be linked to the severity categorization scheme.

5.4 Failure Tolerance

The supplier shall prove the capability of the design to sustain single or multiple failures according to AD-1 sections 5.2.1.3 “Failure Tolerance” and 5.2.1.4 “Exceptions to Failure Tolerance Approach.”

5.5 Failure Propagation

Hardware or software failures shall not propagate to cause additional failures or the hazardous operation of interfacing hardware according to AD-1 section 5.2.1.5 “Failure Propagation.”

5.6 Dependability Analyses

Any reduction/optimization in the analysis required below, shall be agreed depending on the criticality of the subsystem/assembly (see AD-1 section 5.2.1.6 “Dependability Analyses.”).
Dependability analyses shall identify common-mode/common-cause failures and failure propagation. The analyses shall be updated for each development milestone.

Failure Modes Effects Analysis (FMEA): The supplier shall perform a FMEA on the functional and physical design as specified in SD-23. The preliminary FMEA shall establish the criticality of each system function, in order to define the reliability requirements (i.e. failure tolerance and software criticality). All potential failure modes shall be identified and classified according to the severity of their consequences. Common-mode and common-cause failures shall be considered.

The following failure modes shall be considered in the FMEA, as a minimum:
- 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)

- Incorrect commands or command sequence;
- Incorrect software functions.

As a result of the FMEA, measures shall be recommended to render such consequences acceptable, and provisions and actions for failure detection and recovery shall be identified. The FMEA shall show that failures do not propagate to the carrier and neighbouring payloads, or to the ground support equipment. Single point failures shall be identified. OTS equipment shall be considered in the FMEA.

Derating Analysis (DA): The supplier shall perform a DA to assure that the stress levels applied to all EEE components are within the limits specified by SD-4. Components exceeding the derating requirements shall be reported to the Customer in the DA report.

Hardware/ Software Interaction Analysis (HSIA): The supplier shall perform a HSIA to assure that the software is designed to react in an acceptable way to hardware failures. The HSIA shall support the FMEA and may be part of it.

Worst-Case Analysis (WCA): The supplier shall perform a WCA at equipment level to demonstrate performance to specifications, under variations of part parameters and environmental conditions.

5.7 Single-Point Failure (SPF)

The retention of SPFs resulting in failure modes of severity category “catastrophic” or “critical” shall be justified to and approved by the Customer.

5.8 Maintainability

The supplier shall identify those items that cannot be checked after integration, that require late servicing, access or replacement, and limited-life items or consumables.

6 SAFETY

6.1 Safety Approach

The supplier shall establish a safety program intended to protect ground personnel, the launch vehicle (including other payloads), ground support equipment, public and private properties and the environment from hazards associated with PROBA3.
The supplier shall apply the launch site and launch safety requirements, and shall comply with the international and national safety regulations.
It is the supplier’s responsibility to evaluate PROBA3 design and operation, to identify the potential safety hazards and hazard control measures, to verify their implementation and to certify that PROBA3 is safe and complies with the applicable safety requirements.
The requirements of SD-2 shall be applicable, with the possibility for tailoring by the prime as described in section 3.7.

6.2 Safety Reviews and Meetings

The supplier shall support the safety review process required by the launcher authority, and any additional safety review or meeting required by the Customer. Safety progress meetings with the Customer shall be part of the overall PROBA3 project meetings.

6.3 Safety Analyses

Safety analyses shall be performed using the requirements of SD-2. The analyses shall be updated for each development milestone.

The supplier shall perform a Hazard Analysis (HA) to identify hazards and hazard scenarios, apply hazard reduction and identify verification methods, and safety-critical items. The requirements in SD-24 shall be applicable.

The supplier shall perform other safety analyses, as required by the launcher authority or the Customer, to support the safety review process. The outcome of these analyses shall be documented in a Safety Analyses Report.

6.4 Safety Design Principles

The supplier shall apply the hazard reduction precedence “elimination or minimization and control of hazards” as defined in SD-2. Failure tolerance is the basic safety requirement used to control hazards. The system shall meet the following failure tolerance requirements:

- No single system failure or single operator error shall have critical or catastrophic consequences.
- No combination of two independent system failures or operator errors shall have catastrophic consequences.
- Safety inhibits shall be independent and verifiable.
- Multiple failures, which result from common–cause or common–mode failure mechanisms, shall be considered as single failures when determining failure tolerance.

6.5 Safety Inhibits

Safety inhibits shall be implemented where required to comply with safety requirements.

6.6 Safe Without Services

When the safe operation of the system depends on externally provided services (i.e. power), the design shall prevent hazards with catastrophic consequences for a period of time to be agreed with the Customer, after the loss of those services.

6.7 Design for Minimum Risk

Hazards that are not controlled with tolerance to multiple failures (i.e. hazards related to mechanisms, structures, pressurized systems, material compatibility and flammability), shall be controlled by the properties and characteristics of the design, which shall provide margins in accordance with the required factors of safety.

6.8 Fracture Control

Where structural failure can have catastrophic or critical consequence, structures, pressure vessels, fasteners and load—bearing paths within mechanisms shall be designed in accordance with SD-6.

6.9 Safety Factors

Structural safety factors shall be applied. The worst credible combination of environmental conditions shall be considered to determine safety margins.

6.10 Materials

Materials selection shall assure that hazards associated with material characteristics (i.e., toxicity, flammability, out-gassing, off-gassing, resistance to radiation, stress corrosion, thermal cycling and degradation, arc tracking, microbiological growth) are either eliminated or controlled according to the requirements of SD-18.

6.11 Hazard Tracking

The supplier shall establish a hazard reporting system for tracking the status of all identified hazards. The system shall be applied for all hazards with potentially catastrophic or critical consequences. The supplier shall report, and provide evidence, that:

- Controls are defined and agreed
- Verification methods are defined and agreed
- Verification is completed

7 EEE COMPONENTS

7.1 General

The requirements of SD-3 shall be applicable, with the possibility for tailoring by the prime as described in section 3.7.

7.2 Programme Plan

The supplier shall prepare an EEE component control plan as a part of the PA&S plan, in accordance with SD-3.

7.3 Component Selection

The supplier shall be responsible for the selection of components that meet the performance, lifetime, stability, radiation, environmental, material, safety, quality, and reliability requirements. Components should be selected from SD-25, or MIL-STD-975H.
The supplier shall maximize the use of European components and of preferred and qualified components, and minimize the number of component types.
In the case non-qualified components are used, preference shall be given to manufacturers that deliver components qualified to similar specifications, and that have the capability of supplying components to the required specification. Approval of these components shall be via a Part Approval Document (PAD) or Request For Approval (RFA).
The supplier shall review the selected components to check their qualification status prior to procurement.

7.4 Components Screening

Safety-critical components used in flight hardware shall comply with the following standards:

- **Integrated circuits** SCC level C, MIL-883 level B, MIL-PRF-38535 Class Q
- **Transistors/ diodes** SCC level C, MIL-PRF-19500 JANTXV
- **Hybrid circuits** SD-7 level C or MIL-PRF-38534 class H
- **Passives** Relevant MIL-ER specifications (MIL-STD-975) Failure rate M.

7.5 Components Approval

All components qualified and screened in accordance with above requirements do not require the Customer approval. If the above requirements are not met, the supplier shall submit a RFA to the Customer.

7.6 Components Listing

The supplier shall submit a Declared Components List (DCL), according to the format given in SD-3, as a preliminary issue at equipment preliminary design review (or equivalent milestone) and for the Customer approval at equipment design review (or equivalent milestone).

7.7 Radiation Tolerance

All flight components susceptible to particle radiation shall be the subject of a radiation analysis. In particular, components sensitive to SEL should be avoided or protected. Devices sensitive to SEU should be protected by EDAC.

7.8 Programmable Devices

The requirements in SD-5 shall be applicable.

7.9 Off-The-Shelf Equipment

The supplier shall review the components used in OTS equipment to verify compliance with the EEE requirements. The review shall consider the used parts list, the derating rules, and the equipment design.

8 MATERIALS, MECHANICAL PARTS AND PROCESSES

8.1 General

The supplier shall be responsible for the selection of materials, mechanical parts and processes and for demonstrating that they are capable of meeting the operating, environmental, physical, chemical, safety, quality and reliability conditions defined in the applicable specifications.
The selection criteria shall ensure that the number of materials, mechanical parts types, and processes is minimized. Materials and mechanical parts that have been successfully used in similar applications shall be preferred.
The supplier shall describe in the PA&S Plan all the activities associated with the selection, testing, inspection, procurement and control of materials, mechanical parts and processes.
The requirements of SD-18 shall be applicable, with the possibility for tailoring by the prime as described in section 3.7.

8.2 Material Approval

Material approval by the Customer shall be via the Declared Materials List (DML).
The data of SD-26 shall be used for the selection of materials with a previous history of space use.

8.3 Materials, Mechanical Parts and Processes Listing

The supplier shall draw up a Declared Materials List (DML), a Declared Mechanical Parts List (DMPL) and a Declared Process List (DPL). The format and content of the lists can be found in SD-18 and SD-8.
Materials with limited-life characteristics shall be highlighted.
Critical processes shall be highlighted.
The DML shall be submitted to the Agency for approval at the design reviews.

8.4 Materials and Mechanical Parts Requirements

a. Materials used for the manufacture of load-carrying elements shall be of aerospace quality and shall be inspected by the manufacturer to assure freedom from defects.

b. Metallic materials used in structural applications shall have a high resistance to Stress Corrosion Cracking (SCC) and be chosen from SD-13.
c. Metallic materials and welds that are not listed in SD-13 or whose SCC resistance is unknown shall be tested and categorized according to the requirements of SD-14.
d. Use of non-metallic materials shall be limited to those having maximum outgassing of 1% or less and maximum volatile condensable content of 0.1% or less, and complying with the outgassing requirements of SD-9.
e. The effects of atomic oxygen shall be assessed on the basis of the orbit parameters and mission duration.
f. Material design allowable stresses shall be derived from MIL-HBK-5H (metallic materials) or MIL-HBK-17F (non-metallic materials), or from other authoritative sources subject to the Agency's approval. Composite structure allowable stresses shall conservatively allow for degradation due to moisture, temperature and process variables.
g. Structural bolts and fasteners shall be procured to national aerospace standards and shall be subject to NDI to verify freedom from defects. NDI shall not be applied to non-structural fasteners such as those for PCB attachment.
h. Aluminium surfaces shall be treated for corrosion protection with a chemical conversion coating if necessary. Mechanical parts made of stainless steel shall be passivated. Mechanical parts made of Titanium alloys shall be anodized.
i. All materials with limited-life characteristics shall be subject to lot/ batch acceptance tests, to be agreed with the Agency, and shall have their date of manufacture and shelf-life expiration date marked on each lot/ batch.
j. Materials that may constitute a safety hazard or can cause contamination are prohibited from being used without prior approval by the Agency. Examples of such materials are: beryllium (including its oxide), cadmium, zinc, pure mercury, radioactive materials, PVC.
k. Materials shall comply with SD-27 for UV radiation and if applicable for particle radiation.
l. Fluid compatibility- materials that will be in contact with an identified fluid shall be compatible with that fluid. If compatibility data is not available, then testing shall be performed according to NASA-STD-6001.

8.5 Processes Requirements

a. Standard processes or known processes previously used in space applications shall be preferred.
b. The supplier shall maximize the use of existing ESA specifications.
c. Critical processes shall be identified by the supplier and reported to the Agency via a critical process list or the DML. Any process that involves critical or catastrophic hazards shall be identified as critical.
d. The requirements in SD-10, SD-11, SD-12, SD-15 shall be applicable.

9 CONFIGURATION MANAGEMENT

The supplier shall establish and implement a system for configuration identification, configuration control, configuration status accounting, and configuration verification, which shall be in effect during the complete PROBA3 life cycle.

The CM program shall be part of the supplier's PA&S Plan and shall be subject to the Customer's approval.
The requirements of SD-20 shall be applicable, with the possibility for tailoring by the prime as described in section 3.7.

10 SOFTWARE PRODUCT ASSURANCE

The requirements of SD-19 shall be applicable with the modifications in this section, with the possibility for tailoring by the prime as described in section 3.7.

- SD-19, section 5.2.5 (Training): Expected Output not required.
- SD-19, section 5.4.1 (Software product assurance planning and control): A separate software PA plan is not required. The contractor shall include the Software PA Plan in the overall PA&S Plan.
- SD-19, section 5.4.2.1: Separate software PA reporting is not required. The contractor shall include the software PA reporting in the PA reporting for the project.
- SD-19, section 6.2.1.4: Not applicable.

11 OFF-THE-SHELF (OTS) EQUIPMENT

The supplier may use OTS equipment (including software) for the PROBA3 design and operations. The PA program planning and implementation approach for this type of equipment or software shall be described in the PA&S Plan.
Depending on the intended use, the following classes of OTS equipment can be identified:

- Equipment developed, built and qualified for other space projects under PA requirements equivalent to the ones of this document (equipment "S")
- Equipment developed and built for commercial, aviation or military applications (equipment "CAM")

The use of OTS equipment shall not lead to the violation of any applicable safety requirement.
OTS equipment of type S shall be preferred.
The decision by the supplier to use CAM equipment shall be conditioned to the criticality of the function to be performed by the equipment.
The request to use CAM equipment shall be submitted to ESA for approval and shall be accompanied by a justification file.
The need for qualification testing of CAM equipment shall be assessed on a case-by-case basis.