ESA PSS-01-30 Issue 2
March 1992

Reliability assurance requirements for ESA space systems

Prepared by:
Product Assurance & Safety Department
European Space Research and Technology Centre
Noordwijk, The Netherlands

Approved by:
The Inspector General, ESA

european space agency / agence spatiale européenne
8-10, rue Mario-Nikis, 75738 PARIS CEDEX, France

Published by ESA Publications Division,
ESTEC, Noordwijk, The Netherlands

Printed in the Netherlands

ESA Price code: E0

ISSN 0379 - 4059

ABSTRACT

This specification defines the reliability assurance requirements which are applicable to ESA space systems.

DOCUMENT CHANGE RECORD

Issue number and date	Sections affected	Remarks
Issue 1 May 1981		
Issue 2	All sections	Document completely revised

TABLE OF CONTENTS

SECTION 1: GENERAL

1.1 SCOPE

This specification defines the reliability assurance requirements which are applicable to ESA space systems.

1.2 APPLICABILITY

The requirements of this specification will be tailored by ESA to fit the needs and constraints of each programme to which they are applied. In each case, the extent and details of application of these requirements will be described in the applicable Statement of Work (SOW).

1.3 APPLICABLE DOCUMENTS

The specifications listed below are directly applicable to this specification to the extent specified herein.

ESA PSS-01-0	Product assurance and safety policy and basic requirements for ESA space systems
ESA PSS-01-10	Product assurance management requirements for ESA space systems
ESA PSS-01-20	Quality assurance requirements for ESA space systems
ESA PSS-01-301	Derating requirements and application rules for electronic components
ESA PSS-01-303	Failure modes, effects and criticality analysis
ESA PSS-01-40	System safety requirements for ESA space systems
ESA PSS-01-50	Maintainability requirements for ESA space systems
ESA PSS-01-401	ESA fracture control requirements
MIL-HDBK-217	Reliability prediction of electronic equipment

1.4 DEFINITIONS

The definitions listed in annex C shall apply.

PAGE INTENTIONALLY LEFT BLANK

SECTION 2: POLICY AND BASIC APPROACH

2.1 ESA RELIABILITY ASSURANCE POLICY

The ESA reliability policy is defined in ESA PSS-01-0 'Product assurance and safety policy and basic requirements for ESA space systems'.

Reliability engineering is principally a design activity, the main objectives of which are to optimise the reliability of the design against competing constraints such as cost and mass.

Reliability assurance is fundamentally an activity to verify that the design complies with the requirements placed on it.

Reliability engineering and reliability assurance are formally linked through the concurrent implementation of design and verification (reliability analysis) activities.

This policy shall be implemented through the systematic, timely and cost-effective application of a reliability assurance programme.

The contractor shall establish and implement a formally controlled and documented reliability assurance programme in accordance with this ESA reliability policy and the contents of this document.

2.2 BASIC APPROACH

(a) Quantitative reliability requirements will be defined by ESA in the system requirements specifications.

b) Reliability requirements additional to this specification may be defined as a consequence of further availability, maintainability or safety requirements applicable to the programme.

(c) Reliability tasks and their implementation shall be considered as an integral part of the design and development processes.

(d) System reliability requirements shall be apportioned to lower levels.

(e) The evaluation of the reliability characteristics of the system and of its elements shall be performed by analysis, review, test and demonstration (as applicable).

(f) For the purposes of reliability asssessment and this specification, ESA space systems shall be considered as an arrangement of hardware, software and human elements in functional paths.

(g) Reliability-critical functional paths shall be identified through analysis; the reliability of the individual elements within the functional paths shall be assured as part of the reliability-critical items control programme through integration, test and operation phases, including maintenance.

(h) Basic reliability shall be achieved by the use of failure-tolerant design and conservative design margins

(i) The verification of the reliability design objectives shall be achieved through reliability prediction, assessment and analysis, including the analysis of failure modes and effects, hardware/software interactions, contingencies and worst case, and through development, qualification and acceptance tests.

(j) The verification of reliability attributes in the design shall be initially by analysis at all system-design levels and later by various methods of compliance verification and demonstration (e.g. functional and reliability tests, evaluation of field data etc.).

SECTION 3: RELIABILITY PROGRAMME MANAGEMENT

3.1 ORGANISATION AND MANAGEMENT

The contractor shall organise Reliability Assurance as an integral part of his Product Assurance discipline. The requirements of ESA PSS-01-10 shall apply.

3.2 RELIABILITY PROGRAMME PLAN

The contractor shall provide, maintain, and implement a Reliability Programme Plan for each design phase, which describes how compliance with the reliability programme requirements will be assured. The plan shall be approved by the Agency.

3.3 DESIGN REVIEWS

The contractor shall ensure that all reliability data for a design review is complete to a level of detail consistent with the objectives of the review and is presented to the reviewing authority in accordance with the project review schedule.

The contractor's reliability organisation shall participate in all design reviews.

The contractor's reliability function shall prepare the documented record of all analyses, predictions and reports performed in accordance with the contract.

All changes shall be assessed for their impact on reliability and a reassessment performed where the CCB considers it necessary.

All recommendations for design improvement shall be fully justified and formal evidence of acceptance or rejection of the recommendation by the contractor's management shall be provided and documented in the Reliability Recommendation Status Log.

3.4 RELIABILITY DATA FILE

The contractor shall maintain a project reliability data file as part of his overall product assurance documentation system. The file shall contain the following as a minimum:

- current reliability analyses, lists, reports and supporting data;
- copies of analyses, lists and reports delivered for milestone reviews;
- supporting analyses (fault trees, mathematical models, computer simulation data etc.);

- the Reliability Recommendation Status Log;
- reliability requirements;
- failure rate (including justification) and risk assessment data;
- action item tracking data;
- minutes of meetings;
- reliability review and reliability audit results;
- reliability-related nonconformances, failures and failure analyses and waivers;
- human error reports;
- document review tracking data;
- reliability requirements compliance data;
- reliability problem data;
- reliability lessons learned and preferred practice data.

ESA shall be allowed access, on request, to the reliability data file during audits and reliability meetings held on the contractor's premises.

3.5 SUBCONTRACTOR CONTROL

General requirements for the control of subcontractors are defined in ESA PSS-01-10. In particular, the contractor shall be responsible for ensuring that elements obtained from subcontractors and suppliers meet the reliability requirements specified for the overall system. The contractor shall provide subcontractors and suppliers with appropriate requirements and guidance.

The level of reliability requirements imposed on subcontractors and suppliers shall be tailored and identified to be consistent with those imposed on the prime contractor.

3.6 RELIABILITY INCORPORATED IN PREVIOUSLY DESIGNED, MANUFACTURED OR FLOWN ELEMENTS

Where the contractor proposes to use hardware or software designed or manufactured on another programme, it shall be his responsibility to demonstrate to the Agency's satisfaction that he has complied with the requirements of this specification.

To this end he shall supply any material requested by the Agency and complete any work required. If such material cannot be supplied then it shall be deemed not to have been done.

3.7 RELIABILITY OF AGENCY FURNISHED PROPERTY

Where the system includes items furnished by the Agency, the contractor shall define the reliability data to be obtained from the Agency. Where the overall reliability requirements of the system cannot be met with the use of such property, the contractor shall inform the Agency of the necessary appropriate action.

3.8 RELIABILITY PROGRAMME TASKS

The contractor shall perform the reliability tasks and activities throughout the programme phases as an integral part of the overall product assurance programme in accordance with ESA PSS-01-10.

A list of these tasks and their relationship with the programme phases is given in Annex A.

3.9 RELIABILITY PROGRAMME DOCUMENTATION

The contractor shall provide the Agency with adequate documentation of the tasks performed throughout the programme. A recommended list of reliability documents is given in Annex B.

3.10 TRAINING

The contractor shall ensure that his reliability staff receive training and indoctrination in new techniques and technologies as required by the project.

PAGE INTENTIONALLY LEFT BLANK

SECTION 4: RELIABILITY TASKS

4.1 INTRODUCTION

The activities performed by the reliability function on ESA programmes includes the establishment of design requirements, various engineering and analysis tasks that assist the systems engineering process, and tasks to verify that the design complies with the requirements. This includes:

(a) Assisting in producing an optimised design which meets the reliability requirements in the design specification;

(b) Apportioning the system reliability requirements to set requirements for subcontractor reliability programmes;

(c) Performing analyses and reviews of the design to assess its reliability, identify reliability-critical functional paths and reliability-critical items, and verify the design;

(d) Supporting the disposition of nonconformances and failures to solve reliability problems and prevent recurrence.

4.2 DESIGN APPROACH

The design approach assumes that the system is designed, qualifed, manufactured, and operated in accordance with the ESA Product Assurance Requirements as defined in ESA PSS-01-0 and its supporting specifications.

For the purpose of reliability analysis, the design shall be considered as hardware, software and human elements arranged in functional paths.

The contractor shall ensure that reliability is built into the design through the use of fault tolerance and design margins. He shall assess the failure characteristics of systems to identify areas of design weakness and propose corrective solutions.

4.3 DESIGN SPECIFICATIONS

The reliability function shall participate in the writing of design specifications. The specifications shall address:

(a) Functional and environmental requirements.

(b) Test requirements including stress levels, test parameters and strategies, and accept/reject criteria;

(c) Design performance margins, derating factors, apportioned reliability requirements and the definition of unacceptable failure consequences (related to severity);

(d) Software and human reliability requirements;

(e) Fault tolerance criteria;

(f) Fault detection, isolation and recovery, and testability/diagnostic requirements;

(g) Protection of interfaces.

Separate reliability requirements shall be prepared by the contractor for his subcontractors. These shall be derived in such a way as to assure compatibility with the requirements placed by ESA on the prime contractor.

4.4 FUNCTIONAL ANALYSIS

Functional analysis (FA) is the systematic identification of the functional elements and paths between elements, external and internal interfaces and constraints of a system, irrespective of the means of accomplishment of those functions, by hardware, software, man, etc. FA is a prerequisite for the correct design of the system including the reliability and safety analysis of it.

Beginning in the conceptual phase, and as a preliminary to the more detailed reliability analyses, the contractor shall perform and document functional analyses on the system to determine for each functional path through the system the effect of the loss of that functional path on system and mission integrity.

FA is characterised as follows:

a) FA shall be used to produce a hierarchical functional model based on a decomposition of the system functions.

b) The functional model shall form the basis of subsequent reliability analysis as well as assisting the development and understanding of the system and its operation.

c) Functional reliability block diagrams, showing the individual functional paths and their conjunctions (depicting redundancy, failure tolerance, etc.) shall be based on the FA.

d) As a result of the FA, reliability-critical functional paths shall be identified as those functional paths whose loss results in failure effect severity 1 or 2 (see Section 4.5).

4.5 FAILURE EFFECT SEVERITY CATEGORIES

Reliability analysis activities, including FA and FMECA, shall use the Failure Effect Severity Categories (FESC) defined below.

In the FMECA, failure modes shall be determined for each element within a functional path. The FESC shall be assigned to each failure mode according to the analyst's assessment of the potential observed failure effect.

Codes denoting a single-point failure, redundancy etc. shall be assigned to each failure effect to aid the overview of the analysis results.

The rules for the use of the FESC and redundancy codes in the FMECA are given in ESA PSS-01-303.

"Loss of system" shall be defined for each programme. It shall generally refer to the irretrievable loss of the system, including all mission products.
"Loss of mission" refers to the irretrievable loss of the mission products alone (such as experiment data, etc.), the system having survived.
"Mission degradation" refers to the loss of a proportion of the mission products.
The definitions (i.e. criteria) for *"Loss of system", "Loss of mission"* and *"Mission degradation"* will be defined in the SOW.

Failure Effect Severity Categories (FESC)

1	Loss of the system
2	Loss of the mission
3	Mission degradation (with possible initiation of contingency action to allow the mission to continue)
4	Unscheduled maintenance or repair

4.6 FAILURE TOLERANCE

A system design shall not allow any single hardware or software failure, or human error, to cause a failure effect with severity category (FESC) of 1 or 2, or to result in catastrophic or critical hazardous consequences (see ESA PSS-01-40);

A system design shall not allow any single operator error, following the occurrence of a hardware or software failure, to cause a failure effect with severity category (FESC) of 1 or 2, or to result in catastrophic or critical hazardous consequences.

Multiple failures resulting from common cause or common mode failures shall be considered as single failures.

4.7 TRADE STUDIES AND DESIGN EVOLUTION

The reliability function shall participate in the studies performed to establish the design from the conceptual stage, including participation in the trade studies, and shall maintain an involvement in design throughout all project phases, including contributions to, and feedback from, integration, test and operations.

The reliability function shall participate in the establishment of the detailed failure-tolerance requirements.

4.8 FUNCTIONAL AND RELIABILITY BLOCK DIAGRAMS

The contractor shall document functional and reliability block diagrams of the system to support his reliability prediction and FMECA.

The functional diagrams shall identify the elements in each functional path, including the parameters necessary to allow an understanding of the system. The diagrams shall clearly indicate where elements are implemented in hardware or software or by human function, and where alternatives or back-up modes are employed.

Each block of the reliability diagrams shall indicate, or provide a reference to, the predicted and apportioned reliability.

4.9 RELIABILITY APPORTIONMENT AND PREDICTION

The contractor shall apportion the systems' reliability requirements to set requirements for subcontractor programmes. These apportionments shall be documented. All predictions shall define the design baseline to which they refer. Working documentation shall be updated as the design changes.

Starting in the conceptual design stage, the contractor shall develop reliability prediction models and predictions for the system. These models and predictions shall be documented and revised as required during the design evolution, and as additional data become available.

Predictions shall be performed in close coordination with Failure Modes, Effects and Criticality Analyses (FMECA) on the same system elements.

The scale, effort and degree of precision of each prediction shall be appropriate to the phase of the project and the intended use of the results.

Final predictions of reliability and safety critical items shall make use of the electrical, thermal and mechanical stresses deduced from analyses as required for the Justification for Retention.

The contractor shall justify fully any cases where he cannot apply a classical statistical approach to reliability prediction. He shall explain his alternative approach to demonstrate that he is proposing an intrinsically reliable design and that safety margins have been chosen to ensure negligible failure probabilities.

The reliability prediction of structural assemblies and pressure vessels shall not be conducted where these assemblies are designed to the ESA Fracture Control Requirements specified in ESA PSS-01-401.

Predictions shall be used for:

(a) Comparing predicted reliability against apportioned reliability within the system to trade alternative design and reliability/maintainability concepts, guide redundancy decisions and to plan a design capable of meeting the project reliability requirements;

(b) Probability of occurrence determination in support of FMECA, FTA and safety-risk analyses;

(c) Preliminary mean-time-between-failure (MTBF) estimation to support maintainability and logistics planning.

4.10 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

The contractor shall perform FMECA of the complete system. The analyses shall determine the effects of failures on the system, the completion of mission objectives, and the need for maintenance. All analyses shall define the design baseline to which they refer. Working documentation shall be updated as the design changes.

The FMECA shall consider system failures arising from hardware failure, software faults and human error (in conjunction with human reliability analyses (HRA)).

FMECA shall be performed in accordance with ESA PSS-01-303. FMECA shall consider the interfaces between:

(a) Functional elements at system, subsystem, equipment and payload levels;

(b) Flight and ground test functions;

(c) Man and machine (in conjunction with HRA);

(c) Hardware and software.

Means for failure detection shall be analysed in the FMECA. The isolation of failures, their recovery and other contingency aspects shall be the subject of a contingency analysis.

FMECA on the detailed design shall uniquely identify the telemetry, command and measurement parameters.

Failure modes in a safety or hazard monitoring system, such as caution and warning, that could cause the system to fail to detect, combat or operate when needed in response to a hazardous event shall be brought to the attention of the safety function.

A hardware/software interaction analysis (HSIA) shall be conducted on the hardware/software interface to identify the software response to hardware failure. The requirements of this analysis are given in ESA PSS-01-303.

The analysis of the man-machine interface shall be coordinated closely with the safety programme through the human reliability analysis (HRA), and the operating hazards analysis defined in ESA PSS-01-40.

FMECA, HRA and HSIA shall be major considerations in design reviews and shall provide criteria and data for other types of analysis, design improvement, operations, manufacturing/integration, testing and safe operations.

FMECA and their revisions shall document the work done in the analyses and be prepared, distributed and reviewed within the contractor's organisation in good time for the decisions and uses they are intended to support, particularly in relation to design reviews.

4.11 VERIFICATION OF REDUNDANCY

All design redundancy shall be fully testable to ensure not only that the primary hardware and software are operating, but also that all backups are working before entering a period of operation where no maintenance is possible. An example is the final integrated system test before launch of an unmanned spacecraft.

Verification of this requirement shall be reported as an annex to, or part of, the FMECA in accordance with ESA PSS-01-303.

4.12 ANALYSIS DATA BASE

The contractor shall use a common data base for analyses and studies on reliability, maintainability and system safety during the course of a project. The primary sources of data for electronic, electrical and electromechanical parts shall be MIL-HDBK-217 and the contract. For other components and assemblies, including those unique to space vehicles, the contractor shall propose alternative data, giving the data sources and a justification for their use.

He shall submit them to ESA for approval.

4.13 IDENTIFICATION AND CONTROL OF RELIABILITY-CRITICAL ITEMS

4.13.1 Reliability-critical items (RCI) and the reliability-critical items list (RCIL)

A reliability-critical item shall be identified as:

a) A configured hardware, software, firmware, or flight or ground control procedure (item), within a functional path whose loss would lead to failure effects of severity 1 or 2;
b) An item that does not meet, or cannot be verified as meeting, one or more of the applicable reliability requirements;
c) An item which is a major driver in the failure potential of the system.

The contractor shall document the reliability-critical items in a reliability-critical items list (RCIL) which shall be subject to ESA approval.

Reliability-critical items shall be ranked in accordance with criteria defined by the contractor, approved by ESA and documented in the RCIL. This ranking shall be used for RCI control.

Risk assessment data (including severity and likelyhood of failure) shall be supplied as required by the risk assessment programme defined in PSS-01-40.

The reliability-critical items list shall be issued to support design and flight-readiness reviews.

4.13.2 Rationale for retention

A rationale for retention (RFR) for each reliability-critical item in the reliability-critical items list, explaining why it cannot be removed from the design, shall be provided for ESA's approval. The RFR shall explain why the each item is reliability-critical and which performance characteristics require monitoring or control in the reliability-critical items control programme.

4.13.3 Reliability-critical items control

Reliability-critical items shall be subject to a reliability-critical items control programme (RCICP) which shall be established and implemented by the contractor through the design, development and operational phases of the project. This requires that the root cause of failure of each reliability-critical item be identified, and appropriate control measures identified and implemented.

These measures include:

- All design, manufacturing and testing documentation that is related to reliability-critical functions, items and procedures shall be identified and marked, and document traceability shall be maintained by document number and issue;
- The reliability function shall be represented on Material Review Boards (MRB), Failure Review Boards (FRB), Configuration Control Boards (CCB) and Test Review Boards (TRB) that are concerned with reliability-critical items;
- The qualification status of all reliability-critical items shall be tracked;
- Assembly, maintenance, servicing, testing and operation of reliability-critical items is monitored for problems affecting the critical characteristics of the items which may arise during operational phase.

The reliability-critical items list and control programme shall be coordinated and integrated with the project and safety critical items control programmes.

4.14 COMMON-MODE AND COMMON-CAUSE FAILURE ANALYSES

The contractor shall perform and document a systematic analysis to identify common-cause and common-mode failures.

The failure of more than one item (component, equipment etc.) as the result of an external influence (e.g. temperature, vibration etc.) is a common-cause failure. The failure of more than one identical item as the result of a failure-initiating condition that is a characteristic of the items (e.g. a manufacturing error) is a common-mode failure.

These analyses shall be conducted on reliability- and safety-critical items only.

4.15 PARTS APPLICATION ANALYSIS

The design shall use EEE parts which are applied at stress levels significantly lower than the maxima specified by the manufacturers. In certain cases other application restrictions also apply. The stress levels required and other application restrictions are specified in ESA PSS-01-301.

The application stress level shall include stresses imposed by failures of other hardware or by software errors if the components in question are required to support the stress thereby imposed to maintain system integrity.

The contractor shall verify compliance in a report which shall list each part used, its specified stress levels, the highest stress level applied during operation, and a comparison with the above-mentioned ESA requirements.

Non-compliances shall be subject to a request for waiver (RFW). ESA reserves the right to reject any such request.

4.16 WORST-CASE ANALYSIS

The design shall take into account parametric variation of its constituent parts and variation of environmental constraints such as temperature and radiation.

For each piece of equipment, it shall be demonstrated by analysis or test (at the contractor's discretion) that in the worst-case operational scenario (which is identified by the contractor), and with the worst-case variation of its component parameters, the equipment continues to perform within specification.

4.17 CONTINGENCY ANALYSIS

The contractor shall conduct an analysis of:

(a) The risk of contingencies in the space system design;

(b) Prevention, containment and limitation of contingencies;

(c) Detection and diagnosis of contingencies;

(d) Recovery from contingencies.

4.18 FAULT TREE ANALYSIS (FTA)

FTA shall be used as a complement to, or substitute for FMECA, if ESA so agrees. One of the criteria used for justifying FTA shall be that the problem under analysis requires a "top-down" methodology in preference to one that is essentially "bottom-up". An example is where a failure has been identified and the various causes need to be determined, such as investigations of in-orbit failures and common-cause failure analyses.

4.19 HUMAN RELIABILITY ANALYSIS (HRA)

4.19.1 General

The contractor shall adopt during the design, development and operational phases of the system life cycle, a systematic approach to the identification and minimisation of human errors that could have a significant effect on the reliability and safety of the system.

All aspects of human performance shall be considered. This shall include, but shall not be limited to, human reliability in routine, disturbed and unforeseen emergency situations. Methods to enhance error recovery shall be explicitly addressed.

Human reliability analysis (HRA) shall be conducted on critical aspects of the design identified, in the first instance, through reliability, maintainability and safety analyses. This will normally mean that HRA is applied to reliability and safety-critical ground and/or flight operational procedures.

4.19.2 Human-reliability modelling

Both qualitative and quantitative modelling of human reliability shall be carried out. The qualitative methods shall address the following:

(a) Specification of human-performance requirements;

(b) Performance of systematic task analyses to identify actions, decision-making and problem-solving functions to be performed by the operator;

(c) Systematic identification of credible operator errors, their underlying causes, consequences and possible recovery mechanisms;

(d) Specification of appropriate error reduction strategies to minimise the occurrence of errors identified in (c);

Because of data limitations, the quantitative analysis of human reliability shall be used primarily for comparing alternative error-reduction strategies and for demonstrating that the levels of risk arising from human error are acceptable compared with other sources of system failure.

4.20 HUMAN-ERROR REPORTING

The contractor shall implement a systematic approach for the reporting of incidents or near-misses arising directly or indirectly from human error. This reporting system shall include methods for establishing the underlying causes of such errors and to provide feedback from operational experience to allow appropriate error-reduction strategies to be implemented.

PAGE INTENTIONALLY LEFT BLANK

SECTION 5: RELIABILITY TESTING, DEMONSTRATION AND DATA COLLECTION.

5.1 RELIABILITY TESTING

The contractor shall test the hardware, software, firmware and operational procedures to evaluate the reliability performance of the system. As necessary, particular reliability engineering tests, including reliability development/growth testing (RDGT) shall be included. In general, testing to verify reliability characteristics shall be conducted in accordance with the reliability- and/or safety-critical items control programme and the programme test plan.

The purpose of reliability testing shall be to:

(a) Verify the capabilities of the design by inducing known failures to check failure tolerance and effectiveness of failure detection and recovery procedures;

(b) Identify failure modes not previously revealed through design review and analysis, including unexpected interactions between components, including software anomalies;

(c) Identify failure modes which reflect deficiencies in workmanship, materials or quality;

(d) Obtain, where appropriate, failure rates and other reliability data and verify the improvement in design reliability and monitor reliability growth;

(e) Validate the capability of the software and hardware, and the human being and the hardware to operate together in accordance with the design specification.

Reliability data gathered during test activities shall be integrated into the data-collection programme.

5.2 RELIABILITY DEMONSTRATION

Where the reliability or safety analyses so require, the contractor shall demonstrate that the reliability of reliability- and/or safety-critical items is in conformance with the requirements. The items tested shall be representative in terms of configuration and quality of flight items. The test programme for such items shall be subject to approval by ESA. For systems containing software, this shall include approval of the operational profile to which the systems will be subjected.

5.3 RELIABILITY-DATA COLLECTION

Contractors responsible for the design and development, and the maintenance of space systems shall make provisions in their programmes for the collection of data related to the failure of any element under their responsibility. Such data shall be obtained in the development phases primarily through the nonconformance and failure/problem-reporting systems, and in the operational phases through the failure report.

The contractor shall provide for the collection and analysis of data on failures, and amount and mode of system use (e.g. stress of hardware, operational profile of software) from his system during operation.

Equipment outage characteristics (failures and corrective action data) and data on the relevant environmental conditions shall be collected. The data base shall be kept up to date with data from current programmes.

ANNEX A
RELATIONSHIP BETWEEN RELIABILITY REQUIREMENTS/ ACTIVITIES AND PROGRAMME PHASES.

CONCEPTUAL PHASE (PHASE A)

In this phase the reliability assurance tasks shall be:

(a) Develop and establish the project reliability policy to fulfil the reliability requirements;
(b) Support concept trades and perform preliminary reliability analyses to identify and compare the reliability-critical aspects of each design option; perform initial availability assessments where required;
(c) Plan the reliability assurance tasks for the project definition phase.

PROJECT DEFINITION PHASE (PHASE B)

In this phase the reliability assurance tasks shall be:

(a) Continue to support the trade studies towards the selection of a preliminary design;
(b) Establish the failure effect severity categories for the project and allocate quantitative reliability requirements to all levels of the system;
(c) Perform the functional analysis, identify reliability-critical functional paths and establish the applicable failure-tolerance requirements;
(d) Perform the reliability analyses and common mode/common cause failure analyses; produce preliminary reliability-critical items list and the rationale(s) for retention;
(e) Plan the reliability assurance tasks for the detailed design and development phase and prepare the draft reliability plan.

DETAILED DESIGN, DEVELOPMENT, MANUFACTURING, INTEGRATION AND TEST PHASE (PHASE C/D)

In this phase the reliability assurance tasks shall be:

(a) Update the functional analysis and perform detailed reliability analyses and reliability/availability simulations as necessary; update all analyses in line with design maturity and test results; provide inputs to perform risk assessment.
(b) Update and refine the reliability-critical items list and the rationale(s) for retention.
(c) Support the identification of key and mandatory inspection points (MIP/KIP), identify critical parameters of reliability-critical items and initiate and monitor the reliability-critical items control programme.
(d) Perform contingency analyses in conjunction with design and operations engineering.
(e) Support Design Reviews and monitor changes for impact on reliability.

(f) Support quality assurance during manufacture, integration and test; support MRB's and FRB's.
(g) Review design and test specifications and procedures.
(h) Review operational procedures to evaluate human reliability problems related to MMI, check compatibility with the assumptions made in preparing the reliability analysis, determine the impact of incompatibilities etc..
(i) Supervise the collection of reliability data.

OPERATIONAL PHASE (PHASE E)

In this phase the reliability assurance tasks shall be:

(a) Support flight readiness reviews.
(b) Support ground and flight operations.
(c) Monitor the design change traffic and its impact on reliability resulting from design evolution.
(d) Investigate reliability related flight anomalies.
(e) Supervise collection of reliability operational data and update trend analysis.

ANNEX B
RECOMMENDED LIST OF CONTRACTOR-GENERATED RELIABILITY DOCUMENTS

The following list covers the contract documentation requirements established by ESA PSS-01-30.

This list is intended to be used as a reliability programme input to the overall contract DRL for each specific procurement where ESA PSS-01-30 is at least partially applicable.

The Agency will use this list to determine what documentation is required for the programme. The precise scheduling of each deliverable (e.g. how many days before a design review is required) will be defined in the DRL for each project.

An assessment must be made to ensure that there is no duplication of contractor generated documentation. In some cases, the Agency may specify, or agree, that two or more documentation items be combined into a single report.

Key to tables

PDR = Preliminary Design Review
CDR = Critical Design Review

A = Approval
I = Information
R = Review

ITEM	PAR. REF.	DUE DATE	ESA ACTION
Reliability Programme Plan	3.2	a. With proposal b. Negotiated changes before contract execution c. Update to include negotiated changes after contract execution	I
Data on previously flown elements	3.6	a. Initial with proposal b. Update before system PDR	A A
Agency furnished property noncompliance report	3.7	Before system PDR	I
Reliability-critical Items list and Rationale for Retention	4.13.2	a. For PDR and CDR b. Update with major changes	A

ITEM	PAR. REF.	DUE DATE	ESA ACTION
Reliability prediction, models, apportionment and availability assessment	4.9	a. Before PDR b. Update as prescribed	R R
Functional and Reliability block diagram reports	4.8	a. Initial, for PDR b. Final, for CDR c. Update with major changes	R R R
Functional analysis	4.4	a. Initial, for PDR b. Final, for CDR	R R
Failure modes, Effects and Criticality Analysis (FMECA)	4.10	a. Initial, for PDR b. Final, for CDR c. Update with major changes	R R R
Common-mode and common-cause failure analysis	4.14	a. Initial, for PDR b. Final, for CDR	R R
Hardware/Software Interaction Analysis (HSIA)	4.10	a. Initial, for PDR b. Final, for CDR	R R
Part application analysis report	4.15	a. Available for CDR b. Updated with design changes	R A

ITEM	PAR. REF.	DUE DATE	ESA ACTION
Worst case analysis	4.16	a. Initial, for CDR b. Update with design changes	R R
Contigency analysis	4.17	a. Initial, for CDR b. Update with design changes	R R
Human error reports	4.20	a. Orally, 24 hours after occurrence b. Initial written report, three working days c. Error analysis and proposed corrective action as generated	I I I

ITEM	PAR. REF.	DUE DATE	ESA ACTION
Fault tree analysis	4.18	a. Initial, for PDR b. Final, for CDR	I I
Human reliability analysis report	4.19	a. Initial, for PDR b. Final, for CDR Thereafter updates following design changes	R
Test plan (reliability critical items)	5.1	a. Review with reliability programme plan b. Review updates as required	I A
Test procedures (reliability critical items)	5.1	Review before each test	R
Test reports (reliability critical items)	5.1	Review after each event	I
Data collection plan	5.3	a. Initial, with Rel. programme plan b. Updates as required	I A
Data collection reports	5.3	a. Periodic reporting with progress reports	I

PAGE INTENTIONALLY LEFT BLANK

ANNEX C DEFINITIONS

CONTINGENCY ANALYSIS

The ameliorating procedure or activities undertaken or to be undertaken when a foreseen undesirable divergence occurs from planned events.

FAILURE MODE, EFFECT AND CRITICALITY ANALYSIS (FMECA)

The systematic investigation of actual or potential single origin fault conditions from observed cause to performance deviation from nominal conditions and the classification of this deviation in terms of the resulting degree of loss of mission objectives.

FAILURE RATE

The number of failures of an item per unit measure of life (cycles, time, events etc. as applicable for the item).

RELIABILITY APPORTIONMENT

The systematic distribution of the desired success probability of an item to its constituent elements in such a way that the composite success probability of these elements is that desired for the item.

RELIABILITY BLOCK DIAGRAMS

A reliability block diagram is a pictorial presentation created from a series of geometrical shapes arranged in a form to represent the functional organisation of a circuit, subsystem or system.

RELIABILITY PREDICTION

For the stated conditions of use, and taking into account the design of an item, the reliability computed from the observed, assessed or extrapolated reliabilities of its elements.

SINGLE-POINT FAILURE

Single-point failures are single failures which by direct action or by initiation of a chain of events, cause the highest level of integration items to cease performing to specification.