

**Jupiter  
Icy  
Moons  
Orbiter**

**Hardware Reliability Assurance  
Requirements**

**DRAFT 1/29/2004**

Document Custodian: T. Heaps

January 29, 2004



# **HARDWARE RELIABILITY ASSURANCE PLAN FOR THE JUPITER ICY MOONS ORBITER (JIMO) PROJECT**

Rev. -  
Date: 1/29/04

**Author:** \_\_\_\_\_  
Tim Heaps  
**JIMO Reliability, Product and Circuit Reliability Group**

**Approval:** \_\_\_\_\_  
Naomi Palmer  
**Group Supervisor, Product and Circuit Reliability Group**

**Approval:** \_\_\_\_\_  
George H. Greanias  
**Office Manager, Reliability Engineering Office**

**Approval:** \_\_\_\_\_  
Sammy Kayali  
**Mission Assurance Manager, Jupiter Icy Moons Orbiter Project**



Jet Propulsion Laboratory  
California Institute of Technology

## **DOCUMENT CHANGE LOG**

<b>Revision</b>	<b>Date</b>	<b>Affected Pages</b>	<b>Reason for Change</b>
-	1/29/04	All	Initial Draft

# TABLE OF CONTENTS

<b>1</b>	<b>HARDWARE RELIABILITY ASSURANCE REQUIREMENTS.....</b>	<b>5</b>
1.1	<i>Introduction .....</i>	5
1.1.1	Purpose .....	5
1.1.2	Scope .....	5
1.1.3	Applicability and Responsibilities .....	5
<b>2</b>	<b>APPLICABLE DOCUMENTS.....</b>	<b>6</b>
2.1	<i>JPL Documents.....</i>	6
2.2	<i>NASA Documents.....</i>	6
<b>3</b>	<b>RELIABILITY ASSURANCE.....</b>	<b>6</b>
3.1	<i>Reliability Analyses Requirements.....</i>	6
3.2	<i>Success Critical Single Point Failure (SPF) .....</i>	7
3.3	<i>Reliability Analyses .....</i>	7
3.3.1	FMECA .....	7
3.3.2	Electrical/Electronic Worst Case Analysis .....	9
3.3.3	Mechanical Worst Case Analysis .....	10
3.3.4	Electrical/Electronic Parts Stress Analysis .....	10
3.3.5	Structural Stress Analysis .....	10
3.3.6	Thermal Stress Analysis .....	10
3.3.7	Single Event Effects Analysis .....	11
3.3.8	Sneak Circuit Analysis .....	11
3.3.9	System and Mechanical Fault Tree Analysis.....	11
3.3.10	Probabilistic Risk Assessment (PRA).....	12
3.3.11	Parameter Trend Analysis (PTA).....	12
3.4	<i>Operating Time Requirements .....</i>	12
3.5	<i>Reliability Assurance IMPLEMENTATION PLAN .....</i>	12
3.5.1	Reliability Assurance Plan.....	12

# **1     HARDWARE RELIABILITY ASSURANCE REQUIREMENTS**

## **1.1   INTRODUCTION**

### **1.1.1   Purpose**

This document establishes the hardware reliability assurance requirements, which when satisfied, will serve as analytical verification that all assemblies and subsystems meet their hardware performance requirements in the intended operating environment. These requirements are intended to assure that adequate consideration is given to reliability during the design and development of the flight hardware (assemblies and system) and that possible sources of reliability risk are identified and eliminated through the design verification process. The use of the word “shall” is intended to identify a provision that is binding and waivable. The use of the word “will” identifies a desired result.

### **1.1.2   Scope**

The hardware reliability assurance requirements and required activities shall apply to each organization, both internal and external to JPL, supplying hardware used for the JIMO Space System. The requirements of this document apply to hardware during all activities involved in design, development, integration, test, and launch.

### **1.1.3   Applicability and Responsibilities**

This document applies to all Space System flight hardware, instruments, and non-flight test and ground support hardware necessary to accomplish the mission. Primary responsibility for the implementation and accomplishment of activities that satisfy the requirements of this section belong to the responsible design agencies and their respective contractors and subcontractors. All hardware developers shall extend these requirements to their subcontractors and suppliers through appropriate contractual documentation.

## **2 APPLICABLE DOCUMENTS**

The following documents, of the issue in effect on the date of invitation for bids, or request for proposal, form a part of this document to the extent specified herein. The Mission Assurance Manager shall resolve any conflict between the referenced document and this document.

### **2.1 JPL DOCUMENTS**

D-5703	Reliability Analyses for Flight Hardware in Design
D-8545	JPL Derating Guidelines
D-58032	Flight Project Practices
D-53052	Category B Waiver Request/Approval Process
982-00029	JIMO Environmental Requirements Document
982-00025	JIMO EEE PARTS Program Requirements
982-35	JIMO Mission Assurance Requirements
JIMOTR-002	JIMO Single Point Failure Policy

### **2.2 NASA DOCUMENTS**

D-15553	NASA Lessons Learned Information System
---------	---

## **3 RELIABILITY ASSURANCE**

### **3.1 RELIABILITY ANALYSES REQUIREMENTS**

Analyses of the hardware design is performed to ensure proper designed-in reliability and consistency with mission requirements and objectives. The analyses will be performed concurrently with the design effort as applicable. Technical adequacy of each analysis shall be verified and approved by JPL independent review. The following reliability analyses shall utilize the methodology described in JPL D-5703 or JPL approved equivalent:

- (a) Failure Modes, Effects, and Criticality Analysis (FMECA)
- (b) Worst Case Analysis (WCA)
- (c) Electrical/Electronic Parts Stress Analysis (PSA)
- (d) Structural Stress Analysis
- (e) Thermal Stress Analysis
- (f) Single Event Effect Analysis (SEEA)
- (g) Sneak Circuit Analysis

- (h) System and Mechanical Fault Tree Analysis (FTA)
- (i) Probabilistic Risk Assessment (PRA)
- (j) Parameter Trend Analysis (PTA)
- (k) EEE Parts Parameter Variation Worst Case database (approved by JPL)

Responsible design agencies internal or external to JPL, shall be responsible for performing, documenting, and updating all of their analyses in accordance with the requirements specified herein. All analyses will be maintained in a current state and reflect the currently approved design.

The responsible agencies shall implement corrective actions to respond to the results of each analysis. The corrective actions shall be documented and submitted to JPL for approval.

For inherited hardware, existing analyses may be satisfactory if applicability is demonstrated by verification that all originally applied requirements, environments, and other bounding conditions envelope the corresponding elements required by the current application. Analyses shall be performed and documented if applicability cannot be demonstrated or analysis has not been performed.

### **3.2 SUCCESS CRITICAL SINGLE POINT FAILURE (SPF)**

The Space System design shall be in compliance with the JIMO Single Point Failure (SPF) Policy (JIMOTR-002). **All system level SPFs shall be identified and documented in a SPF list.**

### **3.3 RELIABILITY ANALYSES**

The following analyses, as applicable, shall be performed for JIMO hardware elements as defined below. A report shall be written to document the method of analyses and the results as outlined in JPL D-5703 including sufficient detail to allow an independent review by an engineer not involved in the design. The report shall include copies of (or reference to) design documentation, definition of part and/or circuit models, and analysis details. The report shall be submitted to JPL for approval.

#### **3.3.1 FMECA**

The main objective of a FMECA (Failure Modes, Effects, Criticality Analysis) is to identify SPFs (Single Point Failures) and to verify that failures will not propagate and damage other hardware. The FMECA is often considered a two part process. The FMEA (failure modes and effects analysis) addresses all postulated part failure modes in a system and the resultant effect on its operation. The CA (criticality) ranks each postulated failure mode according to the criticality of the effect on system operation

and the probability of its occurrence. A functional FMECA is performed at the functional block level and assists in identification of the impact of lower level failures on system operation. A lower level interface FMECA addresses failure propagation across fault isolation boundaries. Both types of FMECAs shall be performed and documented to analyze postulated failures and identify the potential resultant effects. Functional FMECAs shall be performed on the Flight hardware configurations. Interface FMECAs shall be performed and documented for all spacecraft interfaces and on any support equipment that interfaces to flight hardware. A hand off review of the associated interface FMECAs shall be performed prior to connection of any flight hardware to support equipment for test.

Functional FMECAs shall, as a minimum:

- (a) Be performed at the functional block level.
- (b) Consider all operational modes.
- (c) Verify that a failure in a redundant system element will be detected by the system.
- (d) Verify that the capability exists to switch to the redundant system element after a failure in the primary element to continue/restore operation.
- (e) Verify that a failure in a non-critical circuit (e.g., telemetry, current monitoring, test interfaces not used in flight) will not affect the performance of a critical function.
- (f) Document the analysis in a report as described in D-5703. The report shall be delivered to JPL for independent review and approval.

Interface FMECAs shall, as a minimum:

- (a) Be performed at the slice and/or assembly level interfaces to the piece part level to verify that a failure in any slice and/or assembly interface circuit cannot propagate to and/or damage the interfacing circuit and/or damage hardware in another fault containment region.
- (b) Verify that failures in ground support or test equipment cannot propagate to and damage the flight hardware. A FMEA analysis is considered sufficient in test configurations.
- (c) Consider all operational modes.
- (d) Verify that the capability exists to switch to the redundant system element after a failure in the primary element to continue/restore operation.
- (e) Verify that a failure in a non-critical circuit (e.g., telemetry, current monitoring, test interfaces not used in flight) will not affect the performance of a critical function.
- (f) Verify that all signals running through cable cutter or other mechanism for interrupting a circuit will not damage the flight hardware or cause a functional failure, and will not propagate a failure or cause damage to circuits in another fault containment region given any combination of signal to signal, signal to ground shorts or opens.
- (g) Document the analysis in a report as described in D-5703. The report shall be delivered to JPL for independent review and approval.

### 3.3.2 Electrical/Electronic Worst Case Analysis

A WCA shall be performed and documented as described in D-5703 for all circuit designs, **including hybrids**, to demonstrate that sufficient operating margins exist for all operating conditions and performance requirements considering the variation of part parameters due to the worst case combination of the following:

- (a) Part case temperature range, based on the JIMO environmental requirements document (982-00029) and adjusted as described in D-5703 (lower qualification temp to upper qualification temp + 10C). If the thermal stress analysis (section 3.3.6) indicates a part temperature outside of this range, the WCA shall be amended to take into account the temperature range predicted by the thermal stress analysis.
- (b) Piece part initial tolerance.
- (c) Part aging for the operating life of the mission including ground test time (assuming maximum part temperatures).
- (d) Radiation effects.
- (e) Special factors such as shock, vibration, or vacuum where such conditions would contribute to variations in the circuit parameters, voltage, frequency, and load variations shall also be included.
- (f) A EEE parts parameter variation database shall be produced by the responsible design organization to document the parameter variations and support the worst case analyses. The database shall be provided to JPL for approval before beginning the worst case analyses.

The analysis shall be an extreme value analysis (EVA) or extreme value with temperature tracking, in that the value for each of the variable parameters (including input variables) shall be set to limits that will drive the output to a maximum (and minimum) and shall consider AC, DC, and transient effects on the circuit. Piece part parametric data obtained from testing will be incorporated into the WCA as appropriate.

Analysis of protective circuitry shall be performed to ensure proper operation if a fault were to occur. (i.e., Assume a fault condition occurred such that the protective circuit is operating and will continue to operate under worst case conditions.)

Electrical noise on power lines, including ground differences, and interface signal lines shall be considered. Power supply switching noise transients and Power On/Off transients shall be included.

The WCAs shall be documented in a report, as described in D-5703, to describe all identifiable deficiencies and performance restrictions. The report shall support independent verification, including schematics and simulation models used in the analyses.

### **3.3.3 Mechanical Worst Case Analysis**

Mechanical worst case analyses shall be performed as described in D-5703, to verify that worst case mechanical tolerances (extreme value analysis) and thermal environments cannot adversely affect the performance of mechanical and/or optical assemblies. The analyses shall verify that the design meets any mechanical design margin requirements. A report shall be written to document the method of analyses and the results as outlined in JPL D-5703 and submitted to JPL for approval.

### **3.3.4 Electrical/Electronic Parts Stress Analysis**

Parts Stress Analyses shall be performed under worst case operating conditions and documented to verify that the applied stress on each piece part does not exceed the derating values established in JPL D-8545. The stress analysis shall utilize the predicted part case temperature until a piece part thermal analysis is done. The stress analysis shall be updated to include the results of the thermal analysis. The analysis shall be documented as described in D-5703 and submitted to JPL for approval.

### **3.3.5 Structural Stress Analysis**

A structural stress analysis shall be performed on mechanical and electromechanical (e.g., actuators) subsystems/assemblies at the slice and subsystem level. The analysis shall verify that effects on the structure due to the dynamic environment (i.e., acceleration, shock, vibration, and acoustic noise), including worst case estimates for design environmental conditions (temperature, radiation) do not exceed the requirements established for those conditions and that the margin requirements are met. The analysis shall be documented per D-5703 in a report submitted to JPL for approval.

### **3.3.6 Thermal Stress Analysis**

The thermal stress analysis shall verify that the thermal environment, including worst case estimates, for all anticipated environmental conditions meets the requirements. Operating Allowable Flight Temperatures (AFT) are the mission temperature limits (including allowance for prediction uncertainties) in a worst-case powered-on operational (operating within functional specifications) mode that the thermal control is designed to maintain for the specified assemblies and subsystems (hot or cold). All temperatures are measured at the thermal control surface (e.g. mounting surface, radiator surface, etc.), as specified by Thermal Engineering. The thermal analysis shall determine temperatures at lower level assemblies and thermal interfaces when operating at AFT and shall determine a part case temperature and address material properties and the effect of thermal cycling on solder joints, conformal coating, and other critical materials. If system operating modes require operation outside the normal AFT (for example in a startup from an un-powered configuration) then the thermal analysis shall be extended to include the worst case conditions. The analysis shall be documented in a report submitted to JPL for approval.

### **3.3.7 Single Event Effects Analysis**

Circuit designs containing parts susceptible to radiation induced Single Event Effects (Single Event Upsets(SEU), Single Event Transients (SET), Single Event Gate Rupture (SEGR), ) shall be analyzed to provide either an assembly SEE rate or SEE probability during each mission phase. The required performance characteristics with respect to SEE during operation shall be as follows:

- (a) Verify that temporary loss of function or loss of data:
  - 1. Does not prevent recovery of full performance.
  - 2. Does not cause a mission critical loss of function.
  - 3. Does not prevent restoring normal operation and function via internal correction methods without ground intervention in the event of an SEE.
- (b) Fault traceability shall be provided in the telemetry stream to the greatest extent practical for all anomalies involving SEEs.
- (c) Irreversible actions shall not occur as the result of a SEE.

The analyses shall be documented in a report and delivered to JPL for approval.

### **3.3.8 Sneak Circuit Analysis**

Safety critical and un-powered or cold spare subsystem interface circuits shall be analyzed to determine if sneak paths exist that could apply power. If sneak paths do exist under worst case conditions, there must be assurance that they will not affect the function of the circuits involved nor cause overstress to any parts or result in a safety hazard. The analyses shall be documented in a report and delivered to JPL for approval.

### **3.3.9 System and Mechanical Fault Tree Analysis**

A Fault Tree Analysis (FTA) shall be performed at the Space system level and on all mechanisms and devices. These analyses shall be analyzed in context of their environment and operation to find all credible ways in which the undesired event can occur. The mechanical FTAs shall address failure modes capable of occurring down to the lowest level piece part.

These analyses shall include an assessment of preventive measures to reduce failure likelihood and alternate modes of operation for mitigating failure effects. The corrective actions may be documented using guidelines in JPL D-5703. The results of these analyses will enable engineering decisions to be made by the cognizant design organization to indicate whether or not additional analysis, testing, inspection, or other steps should be taken to increase the reliability of the flight hardware. These decisions shall be reported at all design reviews subsequent to completing the analysis. The analysis, including corrective actions, shall be documented as described in JPL D-5703 and submitted to JPL for approval.

### **3.3.10 Probabilistic Risk Assessment (PRA)**

A space system level Probabilistic Risk Assessment (PRA) shall be used to track relative risk levels throughout the life cycle of the program and shall address all critical events occurring during the mission. The PRA shall be documented in accordance with JPL D-5703 and submitted to JPL for approval. The PRA will be developed at an early stage of the project and the updated PRA presented for review at all major project reviews to support technical risk assessment.

### **3.3.11 Parameter Trend Analysis (PTA)**

Any limited life or consumable item used in flight shall be examined for possible parameter trend measurement opportunities to support long term performance analysis. Decisions made pre-launch and during the mission can be aided by a Parameter Trend Analysis (PTA). If the mean life expectancy is less than five mission lifetimes, the consumable is a candidate for PTA. Parameter Trend Analysis (PTA) shall be used as described in D-5703 to track all key performance parameters selected for monitoring. Adequate monitor points shall be provided for the selected parameters and a prediction methodology shall be defined mathematically to identify significant variation in parameter trending data. The data collected shall be documented and periodic reports presented for review at JPL to identify instances of premature aging to the project for possible action.

## **3.4 OPERATING TIME REQUIREMENTS**

Cumulative test operating time shall be tracked on flight hardware. Flight hardware includes all spares that may be used as flight units and any flight hardware intended for use as a redundant backup, either powered or un-powered in flight. All flight hardware shall have accumulated a minimum of 500 hours (goal of 1000 hours) of operating time prior to delivery to ATLO. All flight hardware shall have a minimum of 1000 hours of operating time (goal of 2000) prior to launch.

## **3.5 RELIABILITY ASSURANCE IMPLEMENTATION PLAN**

### **3.5.1 Reliability Assurance Plan**

A Reliability Assurance Plan shall be developed consistent with this document. The Reliability Assurance Plan shall cover all reliability assurance activities of partners, contractors, and sub-contractors supplying any hardware or ground support equipment. The plan shall be submitted to JPL for review and approval.