Rev.	ECO	Description	Checked	Approval	Date
01	43-005	Initial Release for Internal Comment	BK		2/27/02

Mission
Safety, Reliability, and Quality Assurance Requirements

Dwg. No. 43-09001
Revision 01

27 February 2002

Massachusetts Institute of Technology
Center for Space Research

Coral Reef Mission

Table of Contents

Preface

Revision 01 of this document is being circulated for comment within MIT.

1 Introduction

1.1 Scope

This plan describes the Product Assurance functions performed on the Coral Reef Mission. It includes the disciplines of Reliability, System Safety, Test, Material & Process Control, Parts Control, Configuration Management, Quality Assurance, Contamination Control, and Software Integrity. These functions apply to the science payload, spacecraft, launch operations, and mission operations.

1.2 Mission Organization

Consistent with the Mission Organization Chart (43-01001) the MIT Mission Development Office (MDO) has the responsibility of establishing a consistent Safety, Reliability, and Quality Assurance program which will be flowed down to the contributing organizations involved with the flight program. Applicable requirements will thus be levied upon the MIT Science Payload development group, the spacecraft provided, the launch provider, and the mission operations organization.

1.3 Flight Hardware Description

The flight hardware consists of a science payload and the spacecraft. The science payload includes the structure, optics, detectors, filters, signal processing, data compression, calibration, power and thermal control for the instrument. The spacecraft provides science payload accommodation, satellite power, attitude determination, attitude control, command and data handling, RF systems, thermal control, and mass memory. Greater detail is included in requirement documents for the science instrument and spacecraft.

1.4 Planning

Comprehensive planning is required to implement effective controls over the Coral Reef Mission. This responsibility extends to all subcontracts and suppliers. Proper planning and continuous monitoring will help to insure control of quality, schedule, and costs.

1.5 Sub-System SR&QA Plans

Detailed Safety, Reliability, and Quality Assurance Plans are required for the science payload, spacecraft, and major subcontracts. These plans must cover flight hardware, software, critical Ground Support Equipment (GSE), and mission operations.

1.6 Flow Down of Requirements

In each organization there must be an established procedure for assuring that SR&QA requirements are properly flowed down to suppliers and subcontractors.

2 QUALITY ASSURANCE

2.1 Quality System

Organizations tasked with software and hardware for the Coral Reef Mission are required to define and implement a quality system that is consistent with the requirements of ANSI/ASQC Q9001-1994. The system is to be documented in a quality manual and/or implementation plan. The systems and plans are subject to review by the MIT Mission Development Office.

2.2 Workmanship Standards

Workmanship requirements are a critical part of preventing reliability and quality problems. Hardware and software developers are encouraged to use their own workmanship standards, provided they achieve the workmanship levels necessary for reliable, successful space flight missions.

2.2.1 NASA Hardware Standards and Handbooks

The NASA documents listed below are examples of requirements for space flight hardware.

• NASA-STD-8739.3:	Requirements for Soldered Electrical Connections
• NASA-STD-8739.4:	Crimping, Interconnecting Cables, Harness, and Wiring
• NHB 5300.4 (3H):	Requirements for Crimping and Wire Wrap
• NHB 5300.4 (3I):	Requirements for Printed Wiring Boards
• NHB 5300.4 (3J):	Requirements for Conformal Coating and Staking of Printed Wiring Boards and Electronic Assemblies
• NHB 5300.4 (3K):	Design Requirements for Rigid Printed Wiring Boards and Assemblies
• NHB 5300.4 (3L):	Requirements for Electrostatic Discharge Control (Excluding electrically initiated explosive devices)

2.2.2 Industry Hardware Standards

- Classification level 3 of IPC-A-610 reflects acceptability of electronic assemblies for space flight.
- Classification level 3 of IPC-A-60 reflects acceptability of Printed Circuit Boards for space flight.

2.2.3 Software Standards

A Software Management Plan and Software Quality Assurance Plan will be required by for instrument, spacecraft, and mission operations software. MIT does **not** consider these activities as primarily off-line, inspection activities, but as integral parts of the software design and coding activities. The plans, most likely based upon industrial work on software methodology, should reflect this orientation.

2.3 Mission Assurance Audits and Reporting

Assurance Status Reports will be part of the regular, monthly report to the MDO and will summarize the status of all assurance activities and report on any discrepancies (including corrective actions) that could affect the performance of the investigation. During all phases of the mission, the MDO must be able to assess the reliability of the mission and understand how the problems are being resolved. In order to do this, hardware and software developers are required to document and report failures to the MDO beginning with initial power-up of any flight subsystem or assembly (including critical GSE). Reporting is to continue until successful closure. In order to ensure that the quality system is working the way it is intended, hardware and software developers are required to plan and conduct audits of their internal mission assurance systems and those of their subcontractors and suppliers, examining documentation (processes, procedures, analyses, reports, etc.), operations and products. Hardware and software developers are required to generate and maintain a report for each audit. A summary of all audit findings should be included in the monthly report. The work activities and operations of the developer’s team, including subcontractors and suppliers, may be evaluated, surveyed, or otherwise inspected by designated representatives from the MDO.

3 REVIEWS

3.1 Peer Reviews

Hardware and software developers are encouraged to focus resources from the beginning and throughout the mission development phase on engineering working-level reviews (peer reviews) to identify and resolve concerns prior to formal, system level reviews. The purpose of all peer reviews is to substantiate a detailed understanding of the design's ability to meet all of its performance and interface requirements, to surface correctable problems early, and to ensure best known practices are used that enhance robustness by avoiding known or predictable problems. The manner in which these reviews are conducted and issues resolved should be documented in the developing organizations Plan.

3.2 Formal Reviews

Unlike the many informal engineering peer reviews that occur during the project life cycle, there are two semiformal reviews focusing on requirements and the mission concept. In addition, several formal system level reviews are required to concentrate on end-to-end mission level technical, safety, reliability, flight operations, ground operations, and programmatic issues.

The Requirements and Design Concept Review is typically held prior to the fully funded start of a mission contributor; it is important that both the MDO and the contributor agree on the requirements, scope, and general approach to be taken before full commitment. Tue Baseline Design Review validates the design at the sub-system interface and requirements level, and all ICD and requirements documentation must be released for this review to occur. Long lead time components are ordered after this review. After the designs are fairly complete, a Manufacture and Verification Planning Review is held. This is primarily a resource scheduling exercise, making sure that all players are fully integrated into the process, that all required documentation and facilities are in place, and the program is well positioned to demonstrate compliance with the end-item requirements.

All formal reviews will be chaired by a representative of the MDO, the Mission Systems Engineer; the vice-chair will be the Mission QA Manager. A representative of the PCRF will always have a place on the board as well as several individuals, completely independent of the mission, selected for their particular expertise in space systems.

3.2.1 Reviews for Flight Hardware

- Requirements and Design Concept Review
- Baseline Design Review
- Manufacture and Verification Planning Review
- Pre-Environmental Test Review
- Pre-Ship Review

3.2.2 Reviews for Mission Operations

- Requirements and Design Concept Review
- Baseline Design Review
- Manufacture and Verification Planning Review
- Operations Readiness Review
- Flight Readiness Review

4 Safety

Hardware and software developers are required to plan and implement a system safety program that identifies and controls hazards to personnel, facilities, support equipment, and the flight system during all stages of the mission development, launch, and operations. The program is to address hazards in the flight hardware, associated software, ground support equipment, and support facilities. Hardware and software developers team's system safety program must meet the system safety requirements stated in the applicable launch range safety regulation. The spacecraft development team will take the lead role in launch site safety.

4.1 Ground Operations Procedure Approval

Hardware and software developers are additionally required to submit, in accordance with an agreed to schedule, all ground operations procedures to be used at the launch facility, for review and approval by the MDO. All hazardous operations, as well as the procedures to control them, are to be identified and highlighted. All launch site procedures are to comply with the applicable launch site safety regulations.

5 DESIGN ASSURANCE

5.1 Electrical, Electromechanical, and Electronic (EEE) Parts

Hardware developers are required to implement an appropriate EEE parts program for space flight hardware. As a guideline, level 2 EEE parts should be selected and processed in accordance with the current revision of GSFC 311-INST-001, "Instructions for EEE Parts Selection, Screening, and Qualification", or an internal procedure that meets these standards. Hardware developers are responsible for verifying that any part used in the mission is flight worthy and is not affected by any GIDEP Alert throughout the mission development cycle. When the MDO requests that hardware developers evaluate these situations and provide risk assessments with necessary plans of action, the developer is required to respond promptly and as fully as necessary to resolve the issue well in advance of completed project milestones that would rule out corrective measures.

5.2 Materials

The hardware developer is required to implement a materials and processes control program beginning with the start of the design. Hardware developers are required to maintain lists and usage records for inorganic and metallic, polymeric, lubricants, and processes. Developers should strongly consider providing printed wiring board coupons to an independent laboratory for destructive physical examination screening. Test results should normally be obtained prior to population of printed wiring boards with flight parts.

5.3 Reliability

Early in the program's preliminary design phase, the hardware developer is required to identify specific reliability concerns and the steps being taken to mitigate them. As a minimum, the hardware developer is to conduct Failure Modes and Effects Analysis (FMEA) to a sufficient level of detail that mission critical failures are identified and dealt with effectively.

Appropriate use of the analytical tools and techniques collectively known as Probabilistic Risk Assessment (PRA) will significantly influence the MDO's final judgement on the mission's overall reliability. These tools can include combinations of FMEA, Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Event Sequence Diagrams (ESD), Master Logic Diagrams (MLD), or Reliability Block Diagrams (RBD). PRA is a systematic, logical, comprehensive discipline that periodically blends use of these tools to quantify risk and maintain a current state of knowledge about risk of failure. Each individual tool provides a graphic representation of a complex thought process, which relates causes to outcomes, either from a deductive or inductive logic reference frame. Used together, the selected tools promote situational awareness regarding probabilities of unwanted consequences and the magnitudes of their possible impacts.

It is required that the integrated spacecraft accumulate 168 hours of error-free operation **prior to** the start of environmental testing. It is anticipated that this requirement will be met during an end-to-end mission operations test and training exercise.

5.4 Contamination

The hardware developers are required to plan and implement a contamination control program consistent with the requirements of the mission. The plan should address all aspects of contamination control throughout the mission, including transportation and launch site processing. The CCDs in the payload will operate at low temperature and as such, are the cold trap for contamination boiling off the spacecraft and science instrument. Volatile condensables on optical surfaces must be minimized.

5.5 Software

Software developers are required to employ a structured program for the development of flight and ground software. The program must address appropriate development life cycle phases such as requirement analysis, design, code, unit tests, integration and build test, performance verification, and maintenance.

6 Verification

Hardware and software developers are required to conduct a verification program to ensure that the spacecraft and instrument meet the Coral Reef Mission requirements. The developers are required to prepare and submit adequate verification documentation including a verification matrix, environmental test matrix and verification procedures to the MDO for review. The ability to assemble complete test histories from detailed verification records is required.