431-RQMT-000174
Revision -
Effective Date: To be provide by CM
Expiration Date: To be provide by CM

DRAFT

Lunar Reconnaissance Orbiter Project

Mission Assurance Requirements

July 22, 2005

National Aeronautics and Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

CM FOREWORD

This document is a Lunar Reconnaissance Orbiter (LRO) Project Configuration Management (CM)-controlled document. Changes to this document require prior approval of the applicable Configuration Control Board (CCB) Chairperson or designee. Proposed changes shall be submitted to the LRO CM Office (CMO), along with supportive material justifying the proposed change. Changes to this document will be made by complete revision.

Questions or comments concerning this document should be addressed to:

LRO Configuration Management Office
Mail Stop 431
Goddard Space Flight Center
Greenbelt, Maryland 20771

Signature Page

Prepared by:

_____ _____
Ronald E. Kolecki Date
LRO Systems Assurance Manager
GSFC/NASA, Code 303

Approved by:

_____ _____
Craig Tooley Date
LRO Project Manager
GSFC/NASA, Code 4301

LUNAR RECONNAISSANCE ORBITER PROJECT

DOCUMENT CHANGE RECORD

REV LEVEL	DESCRIPTION OF CHANGE	APPROVED BY	DATE APPROVED

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

LIST OF FIGURES

LIST OF TABLES

LIST OF TABLES (CONTINUED)

Table Page

LIST OF TABLES (CONTINUED)

i PREFACE: LUNAR RECONNAISSANCE ORBITER PROJECT DESCRIPTION

i.i INTRODUCTION

The National Aeronautics and Space Administration's (NASA's) Vision for Space Exploration has the fundamental goal of advancing scientific, security, and economic interests through a robust space exploration program. To help fulfill this vision, NASA will initiate a series of robotic missions to the Moon to prepare for and support future human exploration activities. The primary purpose of the robotic preparation is to reduce risk, enhance mission success, and reduce the cost of future human missions. These objectives will be accomplished by designing and implementing a lunar program of robotic missions to collect critical measurements, demonstrate key technologies, and emplace essential infrastructure. That program is the Robotic Lunar Exploration Program (RLEP).

The RLEP was formed on February 11, 2004, in response to a memorandum received from the Associate Administrator for Space Science, dated February 11, 2004, which assigned management responsibility of the RLEP to the Goddard Space Flight Center (GSFC) and requested the establishment of a dedicated program office to manage this new program. This memorandum was in direct response to the President's Vision for United States (U.S.) Space Exploration ("A Renewed Spirit of Discovery" policy statement) issued in January 2004. In order to support the early Exploration milestones, NASA has directed that the Program Office begin planning and definition work for the early missions.

i.ii PROGRAM OVERVIEW

The RLEP consists of a series of robotic lunar exploration missions, launched on approximately an annual basis, starting no later than 2008. These missions are envisioned to be 'Discovery-class' in scope (i.e., approximately $400M, FY05 dollars, in total mission costs, progressing from phases A through E), and are designed to prepare for and support future human exploration activities. The program is managed by the RLEP office at GSFC.

The RLEP has a broad range of mission content, ranging from remote sensing of the lunar surface, assessment of lunar environment on human health, prospecting for in-situ resources, supporting technology maturation for manned Exploration systems, to the emplacement of infrastructure for manned activities. The series of robotic missions will progress from precursor mission activities for extended duration operations, to long duration operations, and ultimately to a sustained presence on the Moon.

The first project defined within the RLEP is chartered to develop the Lunar Reconnaissance Orbiter (LRO). This mission is to fly in 2008. The second project to be defined is chartered to develop a lunar landed element to be flown in 2009. Subsequent missions will be developed in conjunction with and in response to requirements still under definition by the Exploration Systems Mission Directorate (ESMD) at NASA Headquarters (HQ).

i.iii PROGRAM OBJECTIVES

The President's Vision for U.S. Exploration laid out the following objectives relative to "Space Exploration Beyond Low Earth Orbit", and specifically to the lunar program:

a. Undertake lunar exploration activities to enable sustained human and robotic exploration of Mars and more distant destinations in the solar system.

b. Starting no later than 2008, initiate a series of robotic missions to the Moon to prepare for and support future human exploration activities.

c. Use lunar exploration activities to further science and to develop and test new approaches, technologies, and systems, including use of lunar and other space resources, ultimately to enable sustained human and robotic exploration of Mars as well as more distant destinations in the solar system.

The Strategy-to-Task-to-Technology (STT) process identified five primary objectives for the RLEP program. These objectives are:

Preparing for safe landing and selecting exploration-relevant sites

An extended-duration mission on the surface of the Moon will focus primarily on global geodetic topography and detailed hazard-scale mapping for site selection and safe landing. Key environmental characteristics must be understood for risk reduction to human missions as well as robotic and human vehicle design. The radiation, thermal, and lighting environments are items of primary interest in preparation for a short stay on the Moon. Lunar polar regions are of particular interest for mapping and environmental characterization since there is the potential for locating water ice resources. As the precursor missions prepare for potentially longer duration missions to other sites on the lunar surface, additional topographic and resource-relevant mapping will be required for site selection and landing safety.

Emplacing infrastructure support

Providing support for the human missions with preparatory and/or coincident placement of communications/navigation, power, and other necessary infrastructure is also a fundamental objective of the precursors. If it is eventually determined that humans must stay for a long time on the surface of the Moon to enable future human exploration of Mars, it is possible that infrastructure for resource extraction and generation would also be required.

Preparing for and assessing the possibility of resource utilization

Currently, the resource of most interest is the potential for water ice at the lunar poles. Lunar robotic precursors will use both orbital and *in-situ* ground truth data to determine whether this water ice actually exists, its accessibility, and abundance. If found, technology demonstrations would be required to validate techniques for extraction of water ice from the lunar surface materials. Oxygen (O_2) in the lunar regolith and surface rocks is also of interest and robotic missions may undertake technology demonstrations for small-scale extraction of O_2. Additional surveying for resources and resource extraction (such as drilling) may be undertaken as part of the human missions. Longer duration stays on the surface will possibly lead to requirements for larger scale resource extraction and processing if it is determined that this is economically beneficial.

Maturing technologies

Through the STT process, a set of critical technologies can be prioritized for investment and when available, can be demonstrated as part of the lunar robotic precursor program. Early technology demonstrations in RLEP include radiation and micrometeorite shielding assessment of materials with low mass atomic constituents that may be used for future missions. Critical components of human environmental monitoring systems can also be tested as a greater understanding of the lunar environment is acquired. It is expected that precision-landing technologies will be required for safe landings of the precursor robotic missions in the desired locations. Additional technology demonstrations such as dust mitigation will aid in Extravehicular Activity (EVA) suit design for humans and demonstration of thermal systems will aid in vehicle design for extreme thermal environments.

Preparing for human-based in-situ science activities

Supporting the highest priority research to be performed by the human missions on the Moon will involve cooperative work between humans and robots during the landed missions to perform key research activities such as life science experiments, highly informed sample selections (including subsurface), and other detailed investigations of the surface and interior of the Moon.

1.0 OVERALL REQUIREMENTS

1.1 DESCRIPTION OF OVERALL REQUIREMENTS

The Systems Safety and Mission Assurance Program is applicable to the project and its associated developers.

The developer is required to plan and implement an organized Systems Safety and Mission Assurance Program that encompasses:

- All flight hardware, either designed/built/provided by the developer or furnished by the GSFC, from project initiation through launch and mission operations.
- The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items including ground test equipment that interfaces with flight hardware or software.
- All software critical for mission success.

Managers of the assurance activities shall have direct access to developer management independent of project management, with the functional freedom and authority to interact with all other elements of the project. Issues requiring project management attention shall be addressed with the developer(s) through the Project Manager(s) and/or Contracting Officer Technical Representative(s) (COTR).

1.2 USE OF MULTI-MISSION OR PREVIOUSLY DESIGNED, FABRICATED OR FLOWN HARDWARE

When hardware that was designed, fabricated, or flown on a previous project is considered to have demonstrated compliance with some or all of the requirements of this document such that certain tasks need not be repeated, the developer shall demonstrate how the hardware complies with these requirements. Given the lack of recent lunar environment flight hardware experience, the developer shall submit substantiating documentation in accordance with Data Item Description (DID) 1-1.

1.3 SURVEILLANCE OF THE DEVELOPER

The work activities, operations, and documentation performed by the developer and/or his suppliers are subject to evaluation, review, audit, and inspection by government-designated representatives from GSFC, the Government Inspection Agency (GIA), or an independent assurance contractor (IAC). GSFC will delegate in-plant responsibilities and authority via a letter of delegation, or the GSFC contract with the IAC.

The developer and/or suppliers shall grant access for NASA and/or NASA representatives to conduct an assessment/survey upon notice. Resources shall be provided to assist with the assessment/survey with minimal disruption to work activities. The developer, upon request, shall

provide government assurance representatives with documents, records, and equipment required to perform their assurance and safety activities. The developer shall also provide the government assurance representative(s) with an acceptable work area within developer facilities.

1.4 CONTRACT DELIVERY REQUIREMENTS LIST

The Contract Delivery Requirements List (CDRL) identifies DIDs describing data deliverable to the GSFC Project Office. A complete list of DIDs may be found in Chapter 17 of this document. The following definitions apply with respect to assurance deliverables:

Deliver for Approval: The GSFC Project approves within the period of time that has been negotiated and specified in the contract before the developer may proceed with associated work.

Deliver for Review: The GSFC Project reviews and may comment within 30 days. The developer may continue with associated work while preparing a response to GSFC comments unless directed to stop.

Deliver for Information: For GSFC Project information only. The developer's associated work schedule is not normally affected.

2.0 QUALITY MANAGEMENT SYSTEM

2.1 GENERAL

The developer shall have a quality management system (QMS) that is compliant with the minimum requirements of American National Standards Institute (ANSI)/International Organization for Standardization (ISO)/American Society for Quality (ASQ) Q9001 or equivalent. The developer's Quality Manual shall be provided in accordance with DID 2-1. Certificates issued to ANSI/ISO/ASQC Q9001:1994 will have a maximum validity of 3 years from the publication date of ANSI/ISO/ASQ Q9001:2000.

2.2 SUPPLEMENTAL QUALITY MANAGEMENT SYSTEM REQUIREMENTS

As mentioned previously, some assurance related activities are not covered by ISO requirements. These activities are identified in the following sections and should supplement the ANSI/ISO/ASQ Q9001 requirements.

2.2.1 Control of Nonconforming Product

The developer shall have a closed loop system for identifying and reporting nonconformances, ensuring that corrective action is implemented to prevent recurrence. The developer will audit and test as applicable to verify adequacy of the corrective action implemented. The system shall include a nonconformance review process, which shall consist of a preliminary review and a Material Review Board (MRB). The project Safety and Mission Assurance (SMA) representative shall sign off on all MRB activity relating to flight hardware or ground support equipment (GSE) that interfaces with flight hardware.

2.2.2 Preliminary Review

The preliminary review process shall be initiated with the identification and documentation of a nonconformance. A preliminary review shall be the initial step performed by developer-appointed personnel to determine if the nonconformance is minor and can readily be processed using the following disposition actions:

a. Scrapped, because the product is not usable for the intended purposes and cannot be economically reworked or repaired.

b. Re-worked, to result in a characteristic that completely conforms to the standards or drawing requirements.

c. Returned to supplier, for rework, repair or replacement.

d. Repaired using a standard repair process previously approved by the MRB and /or government Quality Assurance (QA) organization.

e. Referred to MRB when the above actions do not apply to the nonconformance.

Note: Preliminary review does not negate the requirement to identify, segregate, document, and report and disposition nonconformances.

2.2.3 Material Review Board

Nonconformances not dispositioned by preliminary review, normally critical and major nonconformances, shall be referred to the MRB for disposition. MRB dispositions shall include scrap, rework, return to supplier, repair by standard or non-standard repair procedures, use-as-is, or request for major waiver. The MRB shall consist of a core team including QA, supplemented with other disciplines brought in as necessary. It shall be chaired by a developer representative responsible for ensuring that MRB actions are performed in compliance with this standard and implemented per developer procedures. This is usually a systems engineering function.

The MRB shall consist of the appropriate functional and project representatives who are needed to ensure timely determination, implementation and close-out of recommended MRB disposition. Safety and quality assurance personnel shall review all MRBs.

At developer/supplier facilities, NASA/Government representatives shall participate in MRB activities as deemed appropriate by Government management or contract, otherwise, the MRB chairperson shall advise the Government of the MRB actions and recommendations. NASA will exercise the prerogative to review and approve all "use-as-is," standard and non-standard repair dispositions before they are initiated.

The MRB process shall investigate, in a timely manner, nonconforming item(s) in sufficient depth to determine proper disposition. For each reported nonconformance, there shall be an investigation and engineering analysis sufficient to determine cause and corrective actions for the nonconformance. Written authorization shall be provided to disposition the nonconformances.

2.2.4 Reporting of Failures

Reporting of failures shall begin as early in the life cycle as possible. Reporting must begin by the first power application at the start of end item acceptance testing or the first operation of a mechanical item. It shall continue through formal acceptance by the GSFC Project Office. Failures shall be reported in accordance with DID 2-2.

Developer review/disposition/approval of failure reports shall be addressed by a Failure Review Board as described in applicable procedure(s) included or referenced in the Quality Manual.

2.2.5 Control of Monitoring and Measuring Devices

Testing and calibration laboratories shall be compliant with the requirements of ISO 17025, "General Requirements for the Competence of Testing and Calibration Laboratories."

2.2.6 New On-orbit Design

New on-orbit design of software and ground station hardware shall be in accordance with original system design specifications and validation processes.

2.2.7 Flow-Down

The supplier's QA and safety programs shall ensure flow-down of requirements to all suppliers, including a process to verify compliance. Specifically, contract review and purchasing processes shall indicate the processes for documenting, communicating, and reviewing requirements with sub-tier suppliers to ensure requirements are met.

Examples include, but are not limited to the following: Technical, Safety, Parts and Materials, Reliability, Quality Assurance, NASA Advisories, Government Industry Data Exchange Program (GIDEP) (Alerts, Safe-Alerts, Problem Advisories, and Agency Action Notices).

The developer shall prepare and update as necessary a requirements verification matrix showing how the requirements are met by all suppliers. (DID 2-3)

3.0 SYSTEM SAFETY REQUIREMENTS

3.1 GENERAL REQUIREMENTS

The system safety program shall be implemented by all spacecraft (SC) and instrument developers for flight hardware, GSE, associated software, and support facilities. The system safety program shall be initiated in the concept phase of design and continue throughout all phases of the mission. GSFC shall certify safety compliance in support of the Pre-Shipment Review (PSR), and again at the Mission Readiness Review (MRR). The system safety program shall accomplish the following:

a. Provide for the early identification and control of hazards to personnel, facilities, support equipment, and the flight system during all stages of project development including design, development, fabrication, test, handling, storage, transportation, and pre-launch activities. The program shall address hazards in the flight hardware, associated software, GSE, operations, and support facilities, and shall conform to the safety review process requirements of NASA-STD-8719.8, "Expendable Launch Vehicle Payloads Safety Review Process Standard."

b. Meets the system safety requirements of AFSPC 91-710, "Range User Requirements Manual."

c. Meets the baseline industrial safety requirements of the institution, AFSPC 91-710 applicable Industry Standards to the extent practical to meet NASA and Office of Safety and Health Administration (OSHA) design and operational needs, and any special contractually imposed mission unique obligations. This should be documented in the contractor's Facility Health and Safety Plan.

Specific safety requirements include the following:

- If a system failure may lead to a catastrophic hazard, the system shall have three inhibits (dual fault tolerant). A catastrophic hazard is defined as: 1) A hazard that could result in a mishap causing fatal injury to personnel, and/or loss of one or more major elements of the flight vehicle or ground facility. 2) A condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or vehicle during the mission.

- If a system failure may lead to a critical hazard, the system shall have two inhibits (single fault tolerant). A critical hazard is defined as: a condition that may cause severe injury or occupational illness, or major property damage to facilities, system, or flight hardware.

- Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" areas of design, and have separate detailed safety requirements that they must meet. Hazard controls related to these areas are

extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.

3.2 SYSTEM SAFETY DELIVERABLES

3.2.1 System Safety Program Plan

The developer shall prepare a System Safety Program Plan (SSPP) (see DID 3-1) which describes in detail, tasks and activities of system safety management and system safety engineering required to identify, evaluate, eliminate and control hazards or reduce the associated risk to a level acceptable throughout the system life cycle.

The approved plan provides a formal basis of understanding between the developer and GSFC Code 302 on how the System Safety Program will be conducted to meet the range safety requirements, including general and specific provisions. The approved plan shall account for all contractually required tasks and responsibilities on an item-by-item basis, and will address the roles and responsibilities of each organization. The SSPP shall specify the hazard analyses required to be performed on flight hardware, GSE, integration and test (I&T) and pre-launch operations.

3.2.2 Safety Requirements Compliance Checklist

The developer shall demonstrate that the payload is in compliance with all safety requirements (or that Problem Failure Reports [PFRs]/waivers have been submitted and approved by GSFC Code 302 and the launch site safety representative). The developer shall document this in the Safety Requirements Compliance Checklist (see DID 3-2). Safety compliance shall be granted via GSFC Code 302 Safety Certification Letter to the Project Manager only after verification that all applicable safety requirements have been met.

3.2.3 Safety Analysis

The developer and GSFC Code 302 shall jointly tailor safety analysis requirements with the Range based on the complexity of the payload. The analyses described in the following sections are provided as examples of typical hazard analysis techniques. The following analysis may be required as part of the required submittal data.

3.2.3.1 Preliminary Hazard Analysis

The purpose of this task is to perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions.

The developer shall perform and document a PHA in accordance with DID 3-3 to obtain an initial risk assessment of a concept or system. Based on the best available data, including mishap data from similar systems and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint.

Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to Range Safety shall be included.

3.2.3.2 Subsystem Hazard Analysis

The purpose of this task is to perform a Subsystem Hazard Analysis (SSHA) to verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents, to identify previously unidentified hazards associated with the design of subsystems (including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem), and to recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels. The developer shall perform an SSHA to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements.

This will include government-furnished equipment (GFE), non-developmental items, and software. Areas to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. The human shall be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct of this analysis. Results shall be documented in the Safety Assessment Report and Missile System Pre-Launch Safety Data Package (MSPSP).

3.2.3.3 System Hazard Analysis

The purpose of this task is to perform and document a System Hazard Analysis (SHA) to verify system compliance with safety requirements contained in system specifications and other applicable documents, to identify previously unidentified hazards associated with the subsystem interfaces and system functional faults, to assess the risk associated with the total system design (including software, and specifically that of the subsystem interfaces), and to recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels. Results shall be documented in the Safety Assessment Report (SAR) and MSPSP.

3.2.3.4 Operations Hazards Analyses

The developer shall prepare an Operations Hazard Analysis (OHA) which describes the hardware and test equipment operations. The OHA shall be prepared in accordance with DID 3-4, demonstrate that the planned I&T activities are compatible with the facility safety requirements, and that any inherent hazards associated with those activities is mitigated to an acceptable level.

GSFC Code 302 is responsible for reviewing and approving the OHA, as well as the organization's test and handling procedures for I&T prior to receiving the hardware at the I&T facility. GSFC Code 302 shall also review all Work Order Authorizations (WOAs). Hazardous WOAs generated during I&T activities require GSFC Code 302 approval. All hazardous operations must be witnessed by GSFC Code 302.

3.2.3.5 Operating and Support Hazard Analysis

The purpose of this task is to perform and document Operating and Support Hazard Analysis (O&SHA) to evaluate activities for hazards or risks introduced into the system during pre-launch processing, and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks.

The SC developer/observatory integrator shall perform and document an O&SHA to examine procedurally controlled activities at the launch site or processing facilities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering the following criteria: the planned system configuration and/or state at each phase of activity, the facility interfaces, the planned environments, the supporting tools or other equipment (including software controlled automatic test equipment, specified for use; operational and/or task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements), and the potential for unplanned events (including hazards introduced by human errors). The human shall be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis. Results shall be documented in the MSPSP.

3.2.3.6 Software Safety

Hazards caused by software will be identified as a part of the nominal hazard analysis process, and their controls will be verified prior to acceptance. Hazard analysis recommendations typically require the software developer to demonstrate that adequate inhibits and/or controls are incorporated to eliminate or mitigate hazards to an acceptable level. Additional independent assessment may be required as dictated by the hazard probability and severity. Section 5.2.2 describes desired software safety activities to meet NASA HQ guidelines.

3.3 SAFETY ASSESSMENT REPORT

The instrument or subsystem developer shall perform and document a comprehensive evaluation of the mishap risk of their instrument or system. This report is used to assist the SC developer/integrator in preparing the MSPSP for submittal to the launch range. This safety assessment report (refer to DID 3-5) shall identify all safety features of the hardware, software, and system design, as well as procedural related hazards present in the system.

It shall include:

a. Safety criteria and methodology used to classify and rank hazards.

b. Results of hazard analyses and tests used to identify hazards in the system.

c. Hazard reports documenting the results of the safety program efforts.

d. List of hazardous materials generated or used in the system.

e. Conclusion with a signed statement that all identified hazards have been eliminated or controlled to an acceptable level.

f. Recommendations applicable to hazards at the interface of their system.

3.4 MISSILE SYSTEM PRELAUNCH SAFETY PACKAGE

The SC developer/observatory integrator shall prepare and submit three progressive iterations of the MSPSP (see DID 3-6) to GSFC Code 302 for review and approval before submittal to the launch range. Early in the project life cycle, the developer shall work with GSFC Code 302 to tailor (as appropriate) safety requirements deemed not applicable to the payload, and then coordinate these with the launch range. Also, starting early in the design phase and continuing throughout the development effort, the developer shall identify hazards associated with the flight system, GSE, and their interfaces that affect personnel, launch vehicle hardware, or the SC. The SARs from the instrument and subsystem developers shall be used as inputs to the MSPSP.

The MSPSP shall include, at a minimum, a detailed description of the payload design sufficient to support hazard analysis results, hazard analysis methodology, and other applicable safety related information. In addition to identifying hazards, the MSPSP shall also identify applicable hazard controls, verifications, and tracking methods for each hazard, to facilitate a "closed loop" process for tracking all hazards to acceptable closure.

The analysis shall be updated as the hardware progresses through the stages of design, fabrication, and test. A list of all hazardous/toxic materials and associated material Safety Data Sheets shall be prepared and included in the final MSPSP, as well as a detailed description of the hazardous and safety critical operations associated with the payload.

The safety assessment shall begin early in the program formulation process and continue throughout all phases of the mission life cycle. The SC/instrument Project Manager shall demonstrate compliance with these requirements, and shall certify to GSFC Code 302 and the launch range, through this MSPSP, that all safety requirements have been met.

3.5 VERIFICATION TRACKING LOG

The SC developer/observatory integrator shall establish a "closed loop" process for tracking all hazards to acceptable closure through the use of a Verification Tracking Log (VTL) (see DID 3-7). The VTL shall be delivered with the final MSPSP and updated regularly as requested until all items are closed. Individual VTL items shall be closed with appropriate documentation verifying the stated hazard control has been implemented, and individual closures shall be complete prior to the first operational use/restraint.

3.6 GROUND OPERATIONS PROCEDURES

The developer shall submit, in accordance with the contract schedule, all ground operations procedures (see DID 3-8) to be used at GSFC facilities, other integration facilities, or the launch site. All hazardous operations, as well as the procedures to control them, shall be identified and

highlighted. All launch site procedures shall comply with the launch site and NASA safety regulations. GSFC Code 302 will review and approval all hazardous procedures before submittal to the launch range.

3.7 SAFETY VARIANCE

When a specific safety requirement cannot be met, the developer shall submit an associated safety variance, per NAS Procedural Requirement (NPR) 8715.3 and DID 3-9 which identifies the hazard and shows the rationale for approval of a variance. The following definitions apply to the safety variance approval policy:

a. Variance: Documented and approved permission to perform some act or operation contrary to established requirements.

b. Deviation: A documented variance that authorizes departure from a particular safety requirement that does not strictly apply or where the intent of the requirement is being met through alternate means that provide an equivalent level of safety with no additional risk. The OSHA requirements (1910 29 Code of Federal Regulations [CFR]) term for deviation is alternate or supplemental standard only when it applies to OSHA requirements.

c. Waiver: A variance that authorizes departure from a specific safety requirement where a special level of risk has been documented and accepted.

All requests for variance will be accompanied by documentation as to why the requirement cannot be met, what risks are involved, alternative means to reduce the hazard or risk, the duration of the variance, and comments from any affected employees or their representatives (if the variance affects personal safety).

3.8 SUPPORT FOR SAFETY MEETINGS

Technical support shall be provided to the Project for Safety Working Group (SWG) meetings, Technical Interface Meetings (TIMs), and technical reviews, as required. The SWG will meet as necessary to review procedures and analyses that contain or examine safety critical functions, or as convened by GSFC Code 302 to discuss any situations that may arise with respect to overall project safety. Meetings are normally held as a sidebar to other reviews and meetings, to minimize extra travel. There is no required number of meetings.

3.9 ORBITAL DEBRIS ASSESSMENT

The developer shall supply an Orbital Debris Assessment (see DID 3-10), or the information required to produce the assessment consistent with NASA Policy Directive (NPD) 8710.3, “Policy for Limiting Orbital Debris Generation,” and NASA Safety Standard (NSS) 1740.14, “Guidelines and Assessment Procedures for Limiting Orbital Debris,” in accordance with the CDRL. Design and safety activities shall take into account the SC’s ability to conform to debris generation requirements.

3.10 LAUNCH SITE SAFETY SUPPORT

The developer shall provide and coordinate manpower requirements necessary for safety support of all operations at the launch site. Range safety is not responsible for project safety support at the launch ranges. Safety support of hazardous I&T operations performed at the launch site needs to be planned and budgeted for by the project.

3.11 MISHAP REPORTING AND INVESTIGATION

Any mishaps, incidents, hazards, and close calls will be reported to on a NASA Form NF1627 or equivalent form, per NPR 8621.1, "NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping."

3.12 MISCELLANEOUS SUBMITTALS FOR RANGE USE

The following list of forms is required by range safety and shall be submitted through GSFC Safety:

- Material Selection List for Plastic Films, Foams, and Adhesive Tapes – (http://rtreport.ksc.nasa.gov/techreports/95report/msf/ms10.html). The list is published in GP-1098, KSC Ground Operations Safety Plan, Volume I, Safety Requirements, and is updated quarterly. Materials are evaluated for electrostatic discharge (ESD), flammability, and compatibility with hypergols. (Ship-60 day to GSFC)

- Radiation forms/analysis – KHB 1860.1 (KSC Ionizing Radiation Protection Program) and KHB 1860.2 (KSC Non-Ionizing Radiation Protection Program) includes forms for ionizing and non-ionizing radiation from Radio Frequency (RF), light, laser, and radioactive sources. Forms must be completed to provide information on the radiation source(s) and the source user(s). Procedures must also be submitted. (Ship-120 days to GSFC)

- Process Waste Questionnaire (PWQ) (Kennedy Space Center [KSC]/Eastern Range Only) – PWQ records all the hazardous materials that are brought to the range with the payload. Specific information on storage, containment, and spill control are required. (Ship- 60 days to KSC/Eastern Test Range [ETR])

- Environmental Impact Statement (EIS) (KSC/Eastern Range Only) – An EIS is required to define the impact of an aborted/terminated launch. (Ship-60 days to KSC/ETR)

4.0 RELIABILITY REQUIREMENTS

4.1 GENERAL

The Reliability Program shall be tailored in order to:

a. Use Probabilistic Risk Assessment (PRA) to assess, manage, and if necessary, quantitatively assess the need to reduce program risk.

b. Demonstrate that redundant functions, including alternative paths and workarounds, are independent to the extent practicable.

c. Demonstrate that the stress applied to parts is not excessive.

d. Identify single failure items/points, their effect on the attainment of mission objectives and possible safety degradation.

e. Show that the reliability design aligns with mission design life and is consistent among the systems, subsystems and components.

f. Identify limited-life items and ensure that special precautions are taken to conserve their useful life for on-orbit operations.

g. Select significant engineering parameters for the performance of trend analysis to identify performance trends during pre-launch activities.

h. Ensure that the design permits easy replacement of parts and components and easy monitoring of redundant paths.

4.2 RELIABILITY REQUIREMENTS

The developer shall generate a Reliability Program Plan (RPP), in accordance with DID 4-1. The RPP shall describe the planned approach for the reliability activities for the project. The plan shall identify the reliability tasks to be performed, and describe how the reliability tasks will be implemented and controlled. The RPP shall discuss the scheduling of reliability tasks relative to project milestones. The plan shall describe the activities that ensure reliability functions are an integral part of the design and development process and that reliability functions interact effectively with other project disciplines (including systems engineering, hardware design and product assurance). The plan shall describe how reliability assessments will be integrated with the design process and other assurance practices to maximize the probability of meeting mission success criteria.

The developer shall describe how reliability assessments will incorporate definitions of failure, as well as alternate and degraded operating modes, that clearly describe acceptable and unacceptable levels of performance. Degraded operating modes will include failure conditions that could be alleviated or reduced significantly by implementing workarounds.

4.3 PROBABILISTIC RISK ASSESSMENT

The developer shall develop a PRA in accordance with DID 4-2. The PRA shall provide a comprehensive, systematic and integrated approach to identifying undesirable events, the scenarios leading to those events (beginning with the initiating event or events), the frequency or likelihood of those events, and the event consequences. The assessment shall be used to assist in identifying pivotal events that may protect against, aggravate or mitigate the resulting consequences.

The PRA shall be comprehensive and balanced, and shall consider all relevant critical factors, including safety of the public, astronauts and pilots, NASA workforce, adverse impacts on the environment, high value equipment and property, national interests, security, etc. The PRA implementation procedures shall reflect and incorporate the results of project risk analysis, including the identification of hazards, risks and recommended controls to manage risk.

4.4 RELIABILITY ANALYSES

Reliability analyses shall be performed concurrently with design so that identified problem areas can be addressed and corrective action(s) taken (if required) in a timely manner.

4.4.1 Failure Modes and Effects Analysis and Critical Items List

A Failure Modes and Effects Analysis (FMEA) shall be performed early in the design phase, in accordance with DID 4-3, to identify system design problems. As additional design information becomes available the FMEA shall be refined. Failure modes shall be assessed at the component interface level. Each failure mode shall be assessed for the effect at that level of analysis, the next higher level and upward. The failure mode shall be assigned a severity category based on the most severe effect caused by a failure. Mission phases (e.g., launch, deployment, on-orbit operation, and retrieval) shall be addressed in the analysis. Severity categories shall be determined in accordance with Table 4-1:

Table 4-1. Severity Categories

Category	Severity Description
1	Catastrophic Failure modes that could result in serious injury, loss of life (flight or ground personnel), or loss of launch vehicle.
1R	Failure modes of identical or equivalent redundant hardware items that could result in Category 1 effects if all failed.
1S	Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.

Category	Severity Description
2	Critical Failure modes that could result in loss of one or more mission objectives as defined by the GSFC project office.
2R	Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed
3	Significant Failure modes that could cause degradation to mission objectives
4	Minor failure modes that could result in insignificant or no loss to mission objectives.

Failure modes resulting in severity categories 1, 1R, 1S or 2 shall be analyzed at a greater depth, to single parts if necessary, to identify the cause of failure.

Results of the FMEA shall be used to evaluate the design relative to requirements (e.g., no single instrument failure will prevent removal of power from the instrument). Identified discrepancies shall be evaluated by management and design groups to determine the need for corrective action.

The FMEA shall analyze redundancies to ensure that redundant paths are isolated or protected such that any single failure that causes the loss of a functional path will not affect the other functional path(s) or the capability to switch operation to that redundant path.

All failure modes that are assigned to Severity Categories 1, 1R, 1S1 and 2, shall be itemized on a Critical Items List (CIL) and maintained with the FMEA Report, see DID 4-3. Rationale for retaining the items shall be included on the CIL. The FMEA and CIL shall be submitted to GSFC in accordance with the Statement of Work (SOW), or as specified by the RPP.

Results of the FMEA, as well as the CIL, shall be presented at all design reviews starting with the Preliminary Design Review (PDR). Presentations shall include comments on how the analysis was used to perform design trade-offs or how the results were taken into consideration when making design or risk management decisions.

4.4.2 Fault Tree Analysis

The developer shall develop a fault tree analysis (FTA) that addresses both mission failures and degraded modes of operation in accordance with the requirements of DID 4-4. Beginning with each undesired state (mission failure or degraded mission), the fault tree shall be expanded to include all credible combinations of events/faults and environments that could lead to the undesired state. Component hardware/software failures, external hardware/software failures and human factors shall be considered in the analysis. The fault tree in itself is not a quantitative model, but becomes a quantitative assessment when combined with quantitative data as part of the PRA.

4.4.3 Parts Stress Analyses

Each application of electrical, electronic, and electromechanical (EEE) parts shall be subjected to stress analyses for conformance with the applicable derating guidelines. The analyses shall be performed at the most stressful values that result from specified performance and environmental requirements (e.g., temperature and voltage) on the assembly or component. The results of the analyses shall be presented at all design reviews starting with the PDR.

The analyses, with summary sheets and updates, shall be submitted to GSFC for review in accordance with DID 4-5.

Presentations shall include comments on how the analysis was used to perform design trade-offs and how the results were taken into consideration when making design or risk management decisions.

4.4.4 Worst Case Scenarios

The developer shall develop a worst case analysis on circuits where failure results in a severity category of 2 or higher and provides data that questions the flightworthiness of the design. Worst case analyses shall be performed in accordance with DID 4-6. The most sensitive design parameters, including those that are subject to variations that could degrade performance, shall be subjected to the analysis. The adequacy of design margins in the electronic circuits, optics, electromechanical and mechanical items shall be demonstrated by analyses, test or both to ensure flightworthiness.

The analyses shall consider all parameters set at worst case limits and worst case environmental stresses for the parameter or operation being evaluated. Depending on mission parameters and parts selection methods, part parameter values for the analyses will typically include:

- Manufacturing variability
- Variability due to temperature
- Aging effects of environment
- Variability due to cumulative radiation

The analyses shall be updated with design changes. The analyses shall be submitted 30 days prior to Critical Design Review (CDR). The results of the analyses shall be presented at all design reviews starting with the PDR. Presentations shall include comments on how the analysis was used to perform design trade-offs and how the results were taken into consideration when making design or risk management decisions.

4.4.5 Reliability Assessments and Predictions

The developer shall perform comparative numerical reliability assessments and/or reliability predictions in accordance with DID 4-7 to:

- Evaluate alternative design concepts, redundancy and cross-strapping approaches and part substitutions.
- Identify the elements of the design that are the greatest detractors of system reliability.
- Identify potential mission limiting elements and components that will require special attention in part selection, testing, environmental isolation and/or special operations.
- Assist in evaluating the ability of the design to achieve the mission life requirement, other reliability goals and requirements as applicable.
- Evaluate the impact of proposed engineering change and waiver requests on reliability.

The developer shall describe the level of detail of a model suitable for performing the intended functions enumerated above. The assessments and updates shall be submitted to GSFC for information in accordance with DID 4-7. The results of any reliability assessment shall be reported at PDR and CDR. Presentations shall include comments on how the analysis was used to perform design trade-offs and how the results were taken into consideration when making design or risk management decisions.

4.5 RELIABILITY ANALYSIS OF TEST DATA

The developer shall fully utilize test information during the normal test program to assess reliability performance and identify potential or existing problem areas.

4.5.1 Trend Analyses

As part of routine system assessment, the developer shall assess all subsystems and components to determine measurable parameters that relate to performance stability. Selected parameters shall be monitored for trends starting at component acceptance testing and continuing during the system I&T phases. The monitoring will be accomplished within the normal test framework; i.e., during functional tests and environmental tests. The developer shall establish a system for recording and analyzing the parameters as well as any changes from the nominal (even if the levels are within specified limits). Trend analysis data shall be reviewed with operational personnel prior to launch, and operational personnel shall continue recording trends throughout the system's mission life. A list of subsystem and components to be assessed, parameters to be monitored, and trend analysis reports shall be maintained and submitted in accordance with the SOW or the RPP, see DID 4-8. The list of parameters to be monitored shall be presented at CDR, and trend analysis reports shall be presented at Pre-Environmental Review (PER) and Flight Readiness Review (FRR).

4.5.2 Analysis of Test Results

The developer shall analyze test information, trend data and failure investigations to evaluate reliability implications. Identified problem areas shall be documented and directed to the attention of developer management for action. This information shall be included in the

developer's progress reports to the Project or in a separate monthly report. Results of analyses shall be presented at design reviews. Presentations shall include comments on how the analysis was used to perform design trade-offs or how the results were taken into consideration when making design or risk management decisions.

4.6 LIMITED-LIFE ITEMS

Limited-life items shall be identified and submitted for approval in accordance with DID 4-9. The list of limited life items shall present definitions, the impact on mission parameters, responsibilities and a list of limited-life items, and shall include data elements as follows:

- Expected life
- Required life
- Duty cycle
- Rationale for selection

The useful life period starts with fabrication and ends with the completion of the final orbital mission.

The list of limited-life items should include selected structures, thermal control surfaces, solar arrays and electromechanical mechanisms. Atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue should be used to identify limited-life thermal control surfaces and structure items. Mechanisms such as batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, gyros, actuators and scan devices should be included when aging, wear, fatigue and lubricant degradation limit their life. Records shall be maintained that allow evaluation of cumulative stress (time and/or cycles) for limited-life items, starting when useful life is initiated and indicating the project activity that stresses the items. The use of an item whose expected life is less than its mission design life shall be approved by GSFC by means of a program waiver.

4.7 RELIABILITY AND MAINTAINABILITY OF GOVERNMENT-FURNISHED EQUIPMENT

When the overall system includes components or other elements furnished by the Government, the developer shall be responsible for identifying, and requesting from the Project Office, adequate reliability data on the items. The data will be used for performing the reliability analyses. When examination of the data or testing by the developer indicates that the reliability of GFE is inconsistent with the reliability requirements of the overall system, the Project Office shall be formally and promptly notified.

5.0 SOFTWARE ASSURANCE REQUIREMENTS

5.1 GENERAL

For the purposes of this section, all references to the developer shall include the prime software developer, as well as any subcontractors tasked in the development process.

5.2 SOFTWARE ASSURANCE

Software Assurance is the planned and systematic set of activities that ensures that software life cycle processes and products conform to requirements, standards, and procedures Institute of Electrical and Electronics Engineers (IEEE) 610.12. As such, software assurance comprises a set of disciplines that strive to improve the overall quality of the product/software while employing risk mitigation techniques. For NASA, these disciplines include Software Quality, Software Safety, Software Reliability, Verification and Verification (V&V), and Independent Verification and Validation (IV&V).

The developer's Software Assurance Program shall address software assurance disciplines and functions for all flight and ground system software. The Software Assurance Program shall apply to software and firmware developed under this contract, including Government off-the-shelf (GOTS) software, modified off-the-shelf (MOTS) software, and commercial off-the-shelf (COTS) software when included in a NASA system.

The developer shall identify a person responsible for directing and managing the Software Assurance Program (e.g., a software assurance manager). The developer shall prepare and maintain a Software Assurance Plan that meets the intent of DID 5-1 and the IEEE Standard 730, "Software Quality Assurance Plans." For smaller projects, this plan may be incorporated in another planning document (e.g., the Software Management Plan).

The developer shall also plan and document software roles and responsibilities, software development processes and procedures, software reviews, software tools, resources, schedules, and deliverables throughout the development life cycle in a Software Management Plan, see DID 5-2. The developer shall document and maintain under configuration control all software requirements in a Software Requirements Specification, see DID 5-5.

5.2.1 Software Quality

The developer shall implement a Software Quality Program to assure the quality of the software products and software processes. The function of software quality assurance assures that the standards, processes, and procedures correctly implemented and appropriate to the project. Software quality control assures adherence to those software requirements, plans, procedures and standards. The software quality discipline shall plan and conduct process and product assurance activities throughout the development life cycle.

Product assurance activities shall be performed to assure:

- Standards and procedures for management, software engineering and software assurance activities are defined.
- All plans (e.g., Configuration Management [CM], Risk Management, Software Management Plan) required by the contract are documented and comply with contractual requirements.
- Standards, design, and code are evaluated for quality and issues.
- All software requirements are documented and traceable from system requirements to design, code and test (i.e., a software requirements traceability matrix).
- Software requirement verification status is updated and maintained via a software requirements verification matrix.
- Formal and acceptance-level software tests are witnessed to assure satisfactory completion and maintenance of test artifacts.
- Software products and related documentation (e.g., Version Description Documents [VDD] and User Guides) have the required content and satisfy their contractual requirements.
- Project documentation, including plans, procedures, reports, schedules and records are reviewed for impact to the quality of the product.
- Software quality metrics are captured, analyzed, and trended to ensure the quality and safety of the software products.

Process assurance activities shall be performed to assure:

- Management, software engineering, and assurance personnel adhere to specified standards and procedures and comply with contractual requirements.
- All plans (e.g., CM, Risk Management, and Software Management Plan) and procedures are implemented according to specified standards and procedures.
- Contract requirements are passed down to any subcontractors, and that the subcontractor's software products satisfy the prime developer's contractual requirements.
- Engineering peer reviews (e.g., design walkthroughs and code inspections) and software milestone reviews are conducted and action items are tracked to closure.
- A software problem reporting system and corrective action process is in place and provides the capability to document, search, and track software problems and anomalies.

- The software is tested to verify compliance with functional and performance requirements.
- Software safety processes and procedures are followed.
- Management, software engineering, and assurance personnel have received proper software assurance training.

5.2.2 Software Safety

The developer shall conduct a Software Safety Program that is integrated with the overall software assurance and systems safety program and is compliant with the software safety requirements of NASA-STD-8719.13. The developer shall document their approach to the Software Safety Program in the System Safety Program Plan (see DID 3-1) or the Software Management Plan (see DID 5-2), as appropriate. The developer shall ensure that software safety requirements are clearly identified, documented, traced and controlled throughout the life cycle. In cases where the developer cannot meet a software safety requirement and/or feels that it is not in the best interest of the project to implement, the developer shall document these items in a deviation/waiver package. The developer shall furnish this deviation/waiver package to the customer for review/disposition.

For software deemed software safety critical, the developer shall identify and document the software safety critical classification of each item in terms of criticality, severity, associated risks, and likelihood of occurrence. Software safety requirements shall also be clearly identified and distinguishable in the software requirements traceability matrix. The developer shall test all software safety critical components on actual hardware to ensure that the safety requirements were sufficiently implemented and that applicable controls are in place to verify all safety conditions.

The developer shall continually monitor, assess, and review the software development efforts for changes that may affect the safety critical classification of the software and as necessary update engineering analyses to reflect these changes.

5.2.3 Software Reliability

The developer shall conduct a Software Reliability Program for incorporating and measuring reliability in the products produced by each process of the life cycle. Software reliability optimizes the software through emphasis on requiring software error prevention, fault detection, isolation, and recovery be built in.

The developer shall document their Software Reliability Program in the Software Management Plan (see DID 5-2) or in a separate Software Reliability Plan (see DID 5-4), as appropriate. The software reliability program shall be tailored to the appropriate level based upon criticality of the software to the mission, software safety criticality, software complexity, size, cost, consequence of failure, and other attributes. Items to be specifically addressed in the plan shall include the

activities to be undertaken to achieve the software reliability requirements, as well as the activities to be undertaken to demonstrate that the software reliability requirements have been verified.

As part of the software reliability program, the developer shall collect, analyze, and track measures that are consistent with IEEE Standard 982.1-1988, "IEEE Standard Dictionary of Measures to Produce Reliable Software." Measurements for evaluating reliability (e.g., defect density, mean-time-to-failure, and code complexity) shall be documented.

5.2.4 Verification and Validation

The developer shall plan and implement a V&V program to ensure that software being developed or maintained satisfies functional, performance, and other requirements at each stage of the development process and that each phase of the development process yields the right product.

To assist in the verification and validation of software requirements, the developer shall document and maintain under configuration control a Software Requirements Verification Matrix. This matrix shall document the flow-down of each requirement to the test case and test method used to verify compliance and the test results. The matrix shall be made available to NASA upon request.

V&V activities shall be performed during each phase of the development process and shall include the following:

- Analysis of system and software requirements allocation, verifiability, testability, completeness and consistency.
- Design and code walkthroughs and/or inspections (i.e., engineering peer reviews).
- Formal reviews.
- Documented test plans and procedures.
- Test planning, execution, and reporting.

5.2.5 Independent Verification and Validation

The developer shall provide all information required for the NASA IV&V effort to NASA IV&V Facility personnel. This includes, but is not limited to, access to all software reviews and reports, contractor plans and procedures, software code, software design documentation, and software problem reporting data. Wherever possible, the developer shall permit electronic access to the required information or furnish soft copies of requested information to NASA IV&V personnel.

The developer shall review and assess all NASA IV&V findings and recommendations. The developer shall forward their assessment of these findings and recommendations to NASA

IV&V personnel accordingly. The developer shall take necessary corrective action based upon their assessment and notify NASA IV&V personnel of this corrective action. The developer shall also notify NASA IV&V personnel of those instances where they chose not to take corrective action. A developer Point of Contact shall be assigned and available to NASA IV&V personnel, as required, for questions, clarification, and status meetings.

5.3 REVIEWS

5.3.1 Software Reviews

The developer shall conduct the following formal software reviews with GSFC personnel in attendance and/or on the review team:

- Software Requirements Review (SWRR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)
- Acceptance Review (AR)

If software is addressed as part of the formal system-level reviews (e.g., Systems Requirements Review [SRR], PDR, or CDR), the developer shall adhere to the review criteria provided by the GSFC Systems Review Office (SRO) (see Section 8).

The developer shall record and maintain minutes and action items from each review. The developer shall respond to Requests for Action (RFAs) and any action items assigned by the review panel and/or the project as a result of each review. The developer will provide a status of all action items and RFAs at subsequent software or system-level reviews.

5.3.2 Engineering Peer Reviews

The developer shall implement a program of engineering peer reviews (e.g., design walkthroughs or code inspections) throughout the software development life cycle to identify and resolve concerns prior to formal system/subsystem level reviews. Peer review teams shall be comprised of technical experts with significant practical experience relevant to the technology and requirements of the software to be reviewed. These reviews shall be commensurate with the scope, complexity, and acceptable risk of the software system/product. Action Items or RFAs from engineering peer reviews shall be recorded, maintained, and tracked throughout the development life cycle.

5.4 SOFTWARE CONFIGURATION MANAGEMENT

The developer shall develop and implement a Software Configuration Management (SCM) system that provides baseline management and control of software requirements, design, source

code, data, and documentation. The developer shall document the SCM system, and associated tools, in a Software Configuration Management Plan (see DID 5-3) or the Software Management Plan (see DID 5-2). The plan shall address configuration identification, configuration control, configuration status accounting, and configuration audits and reviews. The SCM Plan may be contained within the developers Configuration Management Plan as is done with LRO SCM.

As part of the SCM, the developer shall employ a source code version control tool (e.g., ClearCase, Starbase) that allows developers to check in/check out current or previous versions of a source file. The developer shall also use a requirements management tool (e.g., Dynamic Object-Oriented Requirements System [DOORS]) to manage the software requirements baseline.

5.5 SOFTWARE PROBLEM REPORTING AND CORRECTIVE ACTION

The developer shall document and implement a process for software problem reporting and corrective action that addresses reporting, analyzing, and tracking software nonconformances throughout the development life cycle.

5.6 GFE, EXISTING AND PURCHASED SOFTWARE

If the developer will be provided software or firmware as GFE, or will use existing or purchased software or COTS, the developer shall ensure that the software meets the functional, performance, and interface requirements placed upon it. The developer shall ensure that the software meets applicable standards, including those for design, code and documentation, or shall secure a GSFC Project waiver to those standards.

5.7 SOFTWARE ASSURANCE STATUS REPORTING

As part of the Project Monthly Status Reports (MSRs), the developer shall include the following software assurance highlights:

- Organization and key personnel changes.
- Assurance accomplishments and resulting software assurance metrics for activities such as, but not limited to, inspection and test, reviews, contractor/subcontractor surveys, and audits.
- Subcontractor assurance accomplishments, including items listed above.
- Trends in software quality metric data (e.g., number of software problem reports, including the number of problem reports opened and closed in that reporting period).
- Significant problems or issues that could affect cost, schedule and/or performance.
- Plans for upcoming software assurance activities.
- Lessons Learned.

5.8 NASA SURVEILLANCE OF SOFTWARE DEVELOPMENT

The developer shall allow NASA representatives and/or their designate/assignee to perform surveillance activities throughout the entire software development life cycle. Insight/oversight activities include, but are not limited to the following:

- The developer shall allow NASA representatives remote electronic access to their software problem reporting system.
- The developer shall provide NASA representatives the necessary software documentation to perform their job (e.g., software management plans, software assurance plans, CM plans, design documentation)
- The developer shall allow NASA representatives to review results and corrective action from process and product audits.
- The developer shall allow NASA representatives to be present at any engineering peer reviews (e.g., code inspections). The NASA representative shall be allowed to submit RFAs or action items for developer consideration.
- The developer shall allow NASA representatives to review the status of all RFAs and action items, as well as their resolution.

6.0 GROUND DATA SYSTEMS ASSURANCE REQUIREMENTS

6.1 GENERAL

Ground Data Systems (GDS) components may include, but are not limited to GDS software, firmware and hardware, ground support elements (simulators, etc.), COTS, databases, key parameter and test checkout software, and any software developed under the project that is related to flight mission operations. These components may be developed in-house entirely by the developer, provided by a sub-developer/subcontractor to the developer, purchased by the government, purchased by the developer, or furnished by other parties including the government.

6.2 QUALITY MANAGEMENT SYSTEM

QMS-related requirements are discussed in Section 2 of this document. It should be noted that the QMS shall be applied to the development and assurance functions for GDS components as well. In all cases, the development effort shall provide evidence (records for GSFC review) as insight to the quality of the developing software, hardware and other GDS components as evidence of application of QMS processes, and as status of assurance problems, safety issues and organizational/personnel changes. Records shall include any corrective actions, relating to GDS development, recommended by QMS audits. The developer will allow NASA audits, when deemed necessary by the Project Manager, to assure compliance of the developer's QMS with ANSI/ISO/ASQ Q9001 and to assure that the QMS is applied to the contracted activities.

6.3 REQUIREMENTS

The developer shall identify, document and maintain GDS requirements that will serve as the basis of the development, implementation, operation and maintenance of the GDS and its components. These requirements may include, but are not limited to functional, performance, reliability, maintainability, safety and test/verification requirements.

The developer shall review and analyze the GDS requirements to assure that they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information. The developer shall work with GSFC and/or other entities as necessary to resolve any problems/issues associated with the GDS requirements.

The developer shall baseline the GDS requirements early in the development effort, specifically in conjunction with a formal requirement review. The developer shall maintain the GDS requirements under configuration control throughout the project life cycle. All changes to the GDS requirements, including those generated both internally and externally, shall be managed by the developer's CCB process and reviewed/approved as applicable by GSFC.

6.4 REVIEWS

Formal reviews are discussed in Section 8 of this document.

The developer shall implement a program of engineering reviews (peer reviews) throughout the development life cycle to identify and resolve concerns prior to formal, system level reviews. The developer shall plan for such engineering working-level reviews such that they are represented on the project's development schedule. For each engineering review, the developer shall identify and document the following:

- Review process.
- Required participants in the reviews.
- Specific criteria/requirements for successful completion.
- Artifact(s)/documentation required for the review.
- Review results.
- Describe how follow-up actions are documented, tracked and controlled.

6.5 ASSURANCE ACTIVITIES

The developer shall perform various assurance-related activities throughout the development life cycle to ensure that the GDS and its components meet GDS requirements. The developer shall initiate these activities as early in the development life cycle as possible, specifically in the concept phase, and continue these activities into the operations and maintenance phase where applicable. Some of these assurance-related activities are applicable to all phases of the life cycle, and shall be conducted throughout the entire life cycle. These activities include but are not limited to Planning, Tracking and Oversight.

6.5.1 Requirements Phase

In addition to the activities mentioned above, specific assurance-related activities that the developer shall perform during the requirements phase include, but are not limited to, the following (**Note**: Some of these activities may be performed prior to this phase or subsequent to this phase where applicable):

- Analyze and refine the requirements to assure they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information.
- Ensure requirements are generated, analyzed, refined, decomposed and allocated to appropriate GDS components through the use of a systems analysis and allocation process. This process shall be used to verify requirements are correct and complete at each level prior to further allocation and decomposition, and to verify them for feasibility and top-level design concept prior to further allocation.

- Establish functional, performance, safety, reliability, maintainability and test/verification requirements for each incremental system (delivery/build) as applicable. This process should assure all requirements are allocated to planned increments prior to the design and development of the increment.

- Manage allocation of new and additional requirements between hardware, software and other components by a change review and control process; and manage the reallocation of existing requirements between hardware, software and other components by a change review and control process.

- Use a defined process to generate, review and allocate interface requirements.

- Maintain a process to provide, ensure and maintain two-way requirements traceability from system specifications to hardware, software and other components that serve as configuration items. This requirement traceability shall be established and documented as early in the life cycle as possible.

- Generate, document and maintain a requirements verification matrix.

- Conduct a requirement review and at the end of each phase of the development process to ensure requirements are complete and testable.

6.5.2 Design Phase

Specific assurance-related activities that the developer shall perform during the design phase include, but are not limited to, the following (**Note**: Some of these activities may be performed prior to this phase as applicable):

- Maintain a process to define, maintain, and document interfaces (both internal and external) within the architecture.

- Allocate and maintain traceability between the GDS architecture/components and the GDS requirements.

- Conduct design walkthroughs and reviews.

- Place design under CM

6.5.3 Implementation Phase

Specific assurance-related activities that the developer shall perform during the implementation phase include but are not limited to the following (**Note**: Some of these activities may be performed prior to this phase as applicable):

- Define and document the components of each build, delivery and/or release.

- Conduct peer reviews/walkthroughs for code.

- Conduct unit testing.
- Conduct reviews and appropriate tests at the end of this development process phase, to ensure that the requirements have been correctly implemented into design, code, documentation and data.
- Allocate and maintain traceability between the GDS architecture/components and the GDS requirements.

6.5.4 Testing Phase

Specific assurance-related activities that the developer shall perform during the test phase include but are not limited to the following (**Note**: Some of these activities may be performed prior to this phase as applicable):

- Plan for and document test related activities early in the development stages of the project in a test plan(s). A separate test plan may be required for each of the various types of testing mentioned above. The plan shall be maintained under configuration control and updated as requirements are changed. All test plans shall be made subject to GSFC review and approval as applicable. The developer's test plans shall include, but are not limited to, the following:
  - Description of the tests to be performed, including the different levels of testing (from units to Computer Software Configuration Items [CSCIs] to subsystem to system-level test), expected test results, personnel responsible for testing, any required support from other organizations and data required for the test(s).
  - GDS components to be tested.
  - Test environment under which the test(s) will be conducted including test facility requirements, special test support tools (i.e., simulators, emulators, etc.) and any special operating conditions required.
  - Requirements Verification Matrix (RVM) documenting traceability of requirements to test cases.
- Generate test procedures that implement the test plans and facilitate the verification and validation of GDS requirements. All test procedures shall be made subject to GSFC review and approval as applicable.
- Maintain a process to ensure that any test tools and test data are qualified prior to use during testing activities.
- Ensure that test personnel attend and participate as necessary in various reviews throughout the life cycle, to include but not limited to requirements, architecture and design reviews.

- Identify and document test readiness criteria for both formal and informal testing activities. Test criteria shall be made subject to GSFC review and approval as applicable.

- Maintain and update the RVM generated earlier in the life cycle to include the status (pass, fail, deferred, etc.) of each requirement throughout the testing phases and various testing activities.

- Test reports should document the validation of requirements, specific tests completed, conformance of the test results to the expected results, the number, type and criticality of any identified discrepancies/nonconformances, identification of the hardware, software and other GDS components tested including version number, etc.

- Document all defects/nonconformances encountered during the testing activities. These defects/nonconformances shall be assessed for criticality, severity, impact, etc. to determine appropriate action and resolution. The developer shall track and report on the status of all defects/nonconformances.

- Identify all nonconformances that impact the developer's ability to meet GDS requirements and document these items in a waiver, which must be reviewed/approved by GSFC as applicable.

- Ensure an independent entity, either internal or external QA representatives/personnel, witness all testing activities as appropriate.

- Ensure and maintain configuration control of the test environment including hardware, software, simulators, test data, databases and other components throughout the test program.

- Assess all changes made to the system architecture and its components to determine the necessity for regression testing. The developer shall conduct regression testing based upon assessed and approved/implemented changes as appropriate.

- Conduct contingency and off-nominal condition testing.

- Conduct pre-test briefings and generate briefing messages where appropriate to facilitate the coordination of various test related activities. Briefing message contents may include, but are not limited to:

  - Test Case/Procedure Name/Number.

  - Purpose of the Test.

  - Testing Dates/Times.

  - Test Participants and required resources (scheduling of lab and station support, data sources (e.g. SC, SC data tape, engineering test unit or SC simulator), software,

hardware and support system configurations (to include release/version numbers where appropriate).

- GDS requirements to be verified.
- Contact list to include names and numbers of test participants.

- Conduct post-pass and post-test debriefings. During these debriefs, the developer shall summarize test results, disposition the test (pass/fail, etc), deviations from test procedures, requirements verified and discrepancy reports generated, etc.
- Conduct mission simulations to validate nominal and contingency mission operating procedures and to provide for operator familiarization training. In order to provide ample time for checkout of operational configurations, it is considered essential that users participate in mission simulations.

6.5.5 Delivery Phase

Specific assurance-related activities that the developer shall perform during the delivery phase include but are not limited to the following (**Note**: Some of these activities may be performed prior to this phase as applicable):

- System delivery letter:
  - Description of hardware and software delivery contents.
  - Build instructions, including the source code, databases and all files required to complete a successful software build.
  - Special operating instructions.
  - List and copy of resolved anomaly reports and change requests.
  - List and copy of unresolved anomaly reports and change requests.
  - Matrix of requirements addressed by this release, including waivers for those requirements not met as appropriate.
  - List of changes to documentation associated with this release.
  - Verification success criteria.
  - Known problems and workarounds.
- Software delivery media.
- Accompanying documentation.

6.6 GFE, COTS, EXISTING AND PURCHASED SOFTWARE

If the developer will be provided software, or will use existing or purchased software and/or COTS products, the developer is responsible for these components meeting all functional, performance and interface requirements. Any significant modification to these components shall be subject to all of the provisions of the developer's QMS and the provisions of this document. Significant modification will be subject to GSFC review and defined by the project and its CCB procedures.

6.6.1 COTS Management

The developer shall identify and maintain traceability of GDS requirements satisfied by COTS products/components and shall document the rationale/justification for the selection of all COTS components contained within the GDS. The developer shall ensure that the CM program covers all COTS/components.

The developer shall demonstrate and document the fulfillment of GDS requirements by COTS products/components via the RVM.

6.7 DATABASES

- The developer shall maintain a process and procedure for database development. The process shall include activities such as internal reviews, walkthroughs, statusing, test, and discrepancy resolution.
- The developer shall utilize a process for the V&V of the database system.
- The developer shall ensure that system/software releases and database releases are configured with one another.
- The developer shall implement CM on the database system to ensure that the database release version is defined and documented, controlled and that the integrity of the data contained within is controlled.

6.8 SECURITY ASSURANCE

- The developer shall conduct a security program to identify and mitigate security risks associated with the GDS and its components. All security risks shall be assessed/analyzed for impact and likelihood of occurrence.
- The security program shall ensure that security requirements are established, documented and implemented during all phases of the software life cycle. Security tasks and activities shall include the addressing of security concerns during reviews, analyses, inspections, testing and audits.

- The developer shall identify and characterize system security vulnerabilities to include analyzing GDS assets/components, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability.

- The developer shall identify and report upon all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security.

- The developer shall ensure that solutions are verified and validated with respect to security.

- The developer shall be compliant with all NASA security related policies, procedures, standards and guidelines as appropriate.

6.9 ELECTROMAGNETIC COMPATIBILITY CONTROL

The developer shall demonstrate that GDS equipment is not affected by electromagnetic compatibility (EMC) problems nor does it pose a threat to other equipment.

6.10 RELIABILITY AND AVAILABILITY

Reliability, availability and maintainability assurance requirements for the GDS and associated components shall include the following:

- Starting in the conceptual design stage the developer shall clearly define, based upon LRO mission success criteria and reliability requirements, levels of performance. The developer shall establish and implement specific design criteria needed to mitigate unacceptable levels of performance. Design criteria shall be accessible for GSFC review.

- Based on the definition of acceptable levels of performance, the developer shall define the following minimum acceptable maintainability parameters:

  - Diagnostic time to detect and fault isolate the defective Line Replacement Unit (LRU).

  - Time required to remove and replace the defective LRU.

  - Time required to complete checkout and restore operational status.

- The developer shall assure that equipment and components obtained from COTS vendors meet allocated requirements and if not, such deficiencies shall be reported to GSFC.

- The developer shall develop and implement specific design criteria to facilitate maintenance or repair actions. In establishing maintainability design criteria that meets the specification, the contractor shall use data obtained from similar system installations. Design criteria shall include design for modularity, optimum accessibility, accurate fault diagnostics, standardization, and commonality. Design criteria shall be accessible for GSFC review.

6.11 SYSTEM SAFETY

The developer shall initiate a safety program to identify and mitigate safety critical GDS components. If any GDS component(s) are identified as safety critical, the developer shall conduct a safety program on those components in compliance with NPR 8715.3, "NASA Safety Manual." For GDS components that are software and deemed as safety critical, the safety program shall be implemented in accordance with NASA-STD-8719.13A, "NASA Software Safety Standard." The developer shall establish and identify procedures and instructions, which will be used to execute all system safety analyses.

7.0 RISK MANAGEMENT REQUIREMENTS

7.1 GENERAL

The Developer shall develop and implement a project-specific Risk Management Plan (RMP) (Section 7.3) as a means to anticipate, mitigate and control risks and to focus project resources to ensure success of the project. The NPR 7120.5, "NASA Program and Project Management Processes and Requirements," is the controlling requirements used in the preparation of this plan. (Refer to DID 7-1)

The primary activities of the Developer Continuous Risk Management (CRM) process are:

a. Search for, locate, identify, and document reliability and quality risks before they become problems.

b. Evaluate, classify, and prioritize all identified reliability and quality risks.

c. Develop and implement risk mitigation strategies, actions, and tasks and assign appropriate resources.

d. Track risk being mitigated; capture risk attributes and mitigation information by collecting data; establish performance metrics; and examine trends, deviations, and anomalies.

e. Control risks by performing: risk close-out, re-planning, contingency planning, or continued tracking and execution of the current plan.

f. Communicate and document (via the risk recording, reporting, and monitoring system) risk information to ensure it is conveyed between all levels of the project.

g. Report on outstanding risk items at all management and design reviews.

The GSFC Project Office, the GSFC SRO (for design reviews only), and the Instrument Developer will agree on what level of detail is appropriate for each review.

All identified reliability and quality risks will be documented and reported on in accordance with the Instrument Developer's Risk Management Plan. Although not all risks will be fully mitigated, all risks shall be addressed with mitigation and acceptance strategies agreed upon at appropriate mission reviews.

7.2 APPLICABLE DOCUMENTS

GPR 1060.2 Management Review and Reporting for Programs and Projects

GPR 8700.4 Integrated Independent Reviews

NPR 5100.4 Federal Acquisition Regulation Supplement

NPR 7120.5 Program and Project Management Processes and Requirements

NPR 8000.4 Risk Management Procedural Requirements

NPR 8715.3 NASA Safety Manual

7.3 RISK MANAGEMENT PLAN

The Developer shall document the project-specific implementation of the CRM process in a RMP in accordance with DID 7-1. Preparation of the RMP is a requirement established by NPR 7120.5 and includes the content shown in NPR 8000.4, "Risk Management Procedural Requirements." The plan shall include risks associated with hardware and software (e.g., technical challenges, new technology qualification, etc.), COTS, system safety, performance, cost and schedule (i.e., programmatic risks). The plan shall identify which tools and techniques will be used to manage the risks.

All identified risks shall be documented and reported in accordance with the project's RMP. Identified risk areas shall be addressed at project status reviews and at Integrated Independent Reviews (GPR 8700.4). Risk status shall be available to all members of the project team for review. Although not all risks will be fully mitigated, all risks shall be addressed with mitigation and acceptance strategies agreed upon at appropriate mission reviews.

7.4 RISK LIST

The developer shall maintain a Risk List throughout the project life cycle, along with programmatic impacts. The list should indicate which risks have the highest probability, which have the highest consequences, and which risks represent the greatest risk to mission success. The list should also identify actions being taken to address each specific risk. The Risk List shall be configuration controlled.

Risk status shall be communicated on a regular basis to the entire project team and customers. Risk status shall be communicated to the Governing Program Management Council (GPMC) through the MSRs.

For each primary risk (those having both high probability and high impact/severity), the Developer shall prepare and maintain the following in the risk sections of the Program/Project Plans:

- Description of the risk, including primary causes and contributors, current mitigation strategy, and information collected for tracking purposes.
- Primary consequences should the undesired event occur.
- Estimate of the probability of occurrence (qualitative or quantitative) together with the uncertainty of the estimate and the effectiveness of any implemented risk mitigation measures.

- Potential additional risk mitigation measures, which shall include a comparison of the cost of risk mitigation versus the cost of occurrence multiplied by the probability of occurrence.

- Characterization of a primary risk as "acceptable" shall be supported by a rationale (with the concurrence of the GPMC) that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

7.5 RISK-BASED ACQUISITION MANAGEMENT

GSFC projects shall incorporate the requirements of the Risk-Based Acquisition Management (RBAM) initiative as part of the CRM process. The purpose of RBAM is to convey NASA's focus on safety and mission success to NASA contractors.

Acquisition planning shall incorporate input from GSFC personnel responsible for safety and mission assurance, health, environmental protection, information technology, export control, and security.

When technical proposals are required as part of requests for proposals for supplies or services, offerors shall be instructed to identify and discuss risk factors and their approach for managing those risk factors (see NFS 1815.201 and NSF 1815.203-72). Where the solicitation requires submission of a Safety and Health Plan (see NFS 1823.7001(c)), safety and health shall be considered in the evaluation process (also see NFS 1815.305).

QA surveillance plans are required and prepared with the SOW for all performance based contracts and, as necessary, for other contracts. Those plans shall reflect a specific surveillance approach that is commensurate with the perceived risk. The plans are general at the outset, but after contract award, contracting officers shall ensure that the plans are revised to reflect the risks associated with the successful proposal (see NFS 1846.401).

8.0 INTEGRATED INDEPENDENT REVIEW REQUIREMENTS

8.1 GENERAL REQUIREMENTS

For each specified review conducted by the GSFC SRO, the developer shall:

a. Develop and organize material for oral presentation to the GSFC review team. Copies of the presentation material will be made available 14 days prior to the scheduled reviews.

b. Support splinter meetings resulting from the review.

c. Produce timely written responses to recommendations and action items resulting from the review.

d. Summarize, as appropriate, the results of the engineering peer reviews conducted by the developer.

8.2 OVERVIEW OF REVIEW ACTIVITY

8.2.1 Mission Reviews

The primary purpose of mission-level Integrated Independent Reviews (IIRs) is to provide expert technical review of the end-to-end mission system in accordance with GPR 8700.4. Through the planned series of IIRs, the Integrated Independent Review Team (IIRT) shall evaluate the adequacy of the planning, design, implementation, and associated processes to safely and successfully accomplish the mission requirements. The IIRs shall be supported by a comprehensive set of engineering peer reviews conducted in accordance with GPR 8700.6.

The IIRT shall also assess programmatic performance and ability to deliver on commitments as documented in the approved Project Plan, Program Plan or Program Commitment Agreement. In addition, the IIRT shall note any observed deficiencies with respect to compliance with NPR 7120.5.

The IIRT shall:

- Assess the compatibility of the mission success criteria, and the acceptability of the risk associated with their accomplishment.
- Assess the technical content, schedule, staffing and cost of the project over the entire life cycle.
- Assess progress/milestone achievement against approved baselines.
- Assess system resource management and margins (e.g. mass, power, propellant).
- Assess technical progress, risks remaining and mitigation plans.

- Assess the safety hazards, and hazard mitigation and control strategies.
- Assess the utilization of past lessons learned and the capture of new knowledge.
- Identify deficiencies from the above assessments and recommend corrective measures.

The Project Manager and IIRT shall utilize the success criteria defined in the guidelines for the subject review as a guide for topics to be addressed during the IIRs. The guidelines are maintained on the System Management Office (SMO) web site at http://smo.gsfc.nasa.gov/. Also available on the SMO website, as a guide to the project in preparing for the review, are the evaluation criteria associated with Key System Management Practices. At the conclusion of each review, the IIRT shall use these criteria as key metrics to trend over the life cycle of the project as a benchmark for comparison with other projects.

The specific mission-level reviews consist of the following:

a. System Concept Review (SCR) – The SCR establishes that the baseline mission requirements are clearly understood, that the requirements for each independent system element have been determined. It also verifies that the currently envisioned system design will fully satisfy those requirements, and will justify readiness to fully flow down requirements to lower levels of the system. In addition, the SRR establishes that planning for remaining project activities is adequate and that there are reasonable expectations that the project will accommodate any imposed constraints and meet success criteria within the allocated resources. Typically the first of the IIRT reviews, the SCR occurs in mid-formulation (early in the definition phase). When appropriate, because of shortened development cycles or other considerations, the SCR can be combined with the SRR. (See the SRO review guidelines on the SMO website).

b. System Requirements Review (SRR) – The SRR establishes that, for the current mission system design, requirements have been formally and fully allocated to all independent flight and ground system elements and, in turn, to their respective subsystems. It also demonstrates that all system requirements will be satisfied. In so doing, the project justifies readiness to proceed with preliminary design. The SRR occurs in the latter stages of formulation (midway in the definition phase). When appropriate, because of shortened development cycles or other considerations, the SCR can be combined with the SRR.

c. Preliminary Design Review (PDR) – By illustrating a credible and tractable design solution that meets all mission requirements, the PDR establishes that the project has completed a credible and acceptable mission formulation, is prepared to proceed with the detailed design, and is on track to complete the flight and ground system development and mission operations within the identified cost and schedule constraints. The PDR is conducted at the end of formulation (end of the definition phase).

d. Critical Design Review (CDR) – The CDR establishes that the maturity of the design and development effort is appropriate to support proceeding with full scale fabrication

activities, that the project is on track to complete the flight and ground system development and mission operations in order to meet mission performance requirements within the identified cost and schedule constraints. The CDR is conducted near the completion of final design and after completion of engineering model evaluations and breadboard development and test.

e. Pre-Environmental Review (PER) – Through the complete and comprehensive evaluation of project status, the PER establishes readiness to proceed with environmental testing of the integrated flight system. It demonstrates that the project is on track to complete the flight and ground system development and mission operations in order to fully meet mission performance requirements within allocated cost and schedule resources. The PER is held after completion of the initial successful comprehensive systems test of the fully-integrated flight system, and prior to initiation of the system level environmental test sequence.

f. Pre-Shipment Review (PSR) – The PSR establishes that all flight and ground system verification activities have been successfully completed and that the system is ready for final processing prior to launch and mission operations. The PSR is conducted prior to shipment of flight system elements to the launch site and after successful completion of all verification activities (including environmental and functional performance testing, and ground system and network compatibility testing).

8.2.2 Instrument Reviews

The Integrated Independent Review Program for each instrument shall generally consist of SRR, PDR, CDR, PER and PSR. Where applicable, the System Review Program (SRP) for identical follow-on instruments shall generally consist of a PER and PSR. Success criteria for the mission-level reviews may be tailored in order to define criteria for these reviews.

The review program for instruments provided by the other NASA Centers that are in-line with mission success shall be tailored as appropriate to meet the requirements set herein.

8.2.3 Spacecraft Reviews

The IIRP for each SC shall generally consist of SRR, PDR, CDR, PER, and PSR. Success criteria for the mission-level reviews may be tailored in order to define criteria for these reviews.

8.2.4 Operations Reviews

The SRP associated with mission operations consists of the Mission Operations Review (MOR) and the Flight Operations Review (FOR). In addition, operations are a major subject of the mission reviews.

a. MOR – The MOR establishes the adequacy of plans and schedules for ground systems and flight operations preparation, to justify readiness to proceed with implementation of the remaining required activities. The MOR is the first of two IIRT reviews held to

examine mission operations status. It is typically held subsequent to completion of detail design and fabrication activity, but prior to initiation of major integration activities of flight or ground-system elements.

b. FOR – The FOR reviews the progress of ground system development and mission operations planning activities. It establishes readiness to proceed with final preparations of ground system elements to support successful launch and mission operations. The FOR is held late in the test flow of the flight system, but prior to the last major interactive test between the flight and ground system elements. The review is conducted before shipment of flight system elements to the launch site.

8.3 PEER REVIEWS

The Developer will implement a program of peer reviews at the component and subsystem levels. The program will, at a minimum, consist of a PDR and a CDR. In addition, packaging reviews will be conducted on all electrical and electromechanical components in the flight system.

The PDR and CDR will evaluate the ability of the component or subsystem to perform nominally under operating and environmental conditions during both testing and flight. The results of parts stress analyses and component packaging reviews, including the results of associated tests and analyses, will be discussed at the component PDRs and CDRs.

The packaging reviews will specifically address the following:

a. Placement, mounting, and interconnection of EEE parts on circuit boards or substrates.

b. Structural support and thermal accommodation of the boards, substrates, and their interconnections in the component design.

c. Provisions for protection of the parts and ease of inspection.

The Developer peer reviews will be conducted by personnel who are not directly responsible for design of the hardware under review. The GSFC Project Office and SRO will be invited to attend the peer reviews, and will be provided ten working days notification.

The peer reviews shall have RFA item recordations which are reviewed and assigned to appropriate personnel at the end of the reviews. The Developer team is required to submit written responses to recommendations and action items resulting from the reviews to GSFC in a timely manner.

The results of the reviews will be documented and the documents will be made available for review.

9.0 DESIGN VERIFICATION REQUIREMENTS

9.1 GENERAL

The developer shall conduct a Verification Program to ensure that the flight system meets the specified mission requirements. The program shall consist of functional demonstrations, analytical investigations, physical measurements and tests that simulate all expected environments. The developer shall provide adequate verification documentation including a verification plan and matrix, environmental test matrix and verification procedures.

The Verification Program begins with functional testing of assemblies. It continues through functional and environmental testing, supported by appropriate analysis at the unit/component, subsystem/instrument and SC/payload levels of assembly. The program concludes with end-to-end testing of the entire operational system including the payload, the Payload Operations Control Center (POCC), and the appropriate GDS elements.

The "General Environmental Verification Standards (GEVS) for Flight Programs and Projects (GSFC-STD-7000)" shall be used as a baseline guide for developing the verification program. The GEVS-SE document is available at: http://msc-docrv.gsfc.nasa.gov/cmdata/170/STD/GEVS-STD-7000.pdf. Alternative methods are acceptable provided that the net result demonstrates compliance with the intent of the requirements.

9.2 DOCUMENTATION REQUIREMENTS

The following documentation requirements shall be tailored to meet project needs, and shall be delivered and approved in accordance with the DIDs associated with this section.

9.2.1 System Performance Verification Plan

A System Performance Verification Plan (see DID 9-1) shall be prepared. It shall define the tasks and methods required to determine the ability of the system to meet each project-level performance requirement (structural, thermal, optical, electrical, guidance/control, RF/telemetry, science, mission operational, etc.) and to measure specification compliance. Limitations in the ability to verify any performance requirement shall be addressed, including the use of supplemental tests and/or analyses that will be performed, and a risk assessment of the inability to verify the requirement.

The plan shall address how compliance with each specification requirement will be verified. If verification relies on the results of measurements and/or analyses performed at lower (or other) levels of assembly, this dependence shall be described.

For each analysis activity, the plan shall include objectives, a description of the mathematical model, assumptions on which the models will be based, required output, criteria for assessing the acceptability of the results, the interaction with related test activity (if any) and requirements for reports. Analysis results shall take into account tolerance build-ups in the parameters being used.

The following sections detail documents that may be included as part of the System Performance Verification Plan or as separate documents to meet project needs.

9.2.2 Environmental Verification Plan

An Environmental Verification Plan shall be prepared, as part of the System Performance Verification Plan or as a separate document, that prescribes the tests and analyses that will collectively demonstrate that the hardware and software comply with the environmental verification requirements.

The Environmental Verification Plan shall provide the overall approach to accomplishing the environmental verification program. For each test, it shall include the level of assembly, the configuration of the item, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, necessary functional operations, personnel responsibilities and requirements for procedures and reports. It shall also define a rationale for retest determination that does not invalidate previous verification activities. When appropriate, the interaction of the test and analysis activities shall be described.

Limitations in the environmental verification program that prevent the verification by test of any system requirement shall be documented. Alternative tests and analyses shall be evaluated and implemented as appropriate, and an assessment of project risk shall be included in the System Performance Verification Plan. Because of the intended tailoring of the verification program, the preliminary plan shall provide sufficient verification philosophy and detail to allow assessment of the program. For example, for the environmental test portion of the verification, it is not sufficient to state that the GSFC GEVS requirements will be met. A program philosophy must be included.

Examples of program philosophy are:

- All components shall be subjected to random vibration. Random vibration shall be performed at the subsystem or section level of assembly rather than at the component level.
- All instruments shall be subjected to acoustics tests and 3-axis sine and random vibration.
- All components shall be subjected to EMC tests.
- All flight hardware shall see 8-thermal-vacuum cycles prior to integration on the SC.

9.2.3 System Performance Verification Matrix

A System Performance Verification Matrix shall be prepared and maintained, to show each specification requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, results, report reference numbers, etc.

This matrix shall be included in the system review data packages showing the current verification status as applicable.

9.2.4 Environmental Test Matrix

As an adjunct to the system/environmental verification plan, an Environmental Test Matrix (ETM) shall be prepared that summarizes all tests to be performed on each component, each subsystem or instrument, and the payload.

The purpose is to provide a ready reference to the contents of the test program in order to prevent the deletion of a portion thereof without an alternative means of accomplishing the objectives. All flight hardware, spares, and prototypes (when appropriate) shall be included in the ETM. The matrix shall be prepared in conjunction with the initial environmental verification plan and shall be updated as changes occur.

A complementary matrix shall be kept showing the tests that have been performed on each component, subsystem, instrument or payload (or other applicable level of assembly). This shall include tests performed on prototypes or engineering units used in the qualification program and shall indicate test results (pass/fail or malfunctions).

9.2.5 Environmental Verification Specification

As part of the System Performance Verification Plan, or as a separate document, an environmental verification specification shall be prepared that defines the specific environmental parameters that each system element is subjected to, either by test or analysis, in order to demonstrate its ability to meet the mission performance requirements. Such things as payload peculiarities and interaction with the launch vehicle shall be taken into account.

9.2.6 Performance Verification Procedures

For each verification test activity conducted at the component, subsystem, and payload levels (or other appropriate levels) of assembly, a verification procedure shall be prepared that describes the configuration of the test article, how each test activity contained in the verification plan and specification will be implemented (see DID 9-2 for guidance).

Test procedures shall contain details such as instrumentation monitoring, facility control sequences, test article functions, test parameters, pass/fail criteria, quality control checkpoints, data collection, and reporting requirements. The procedures also shall address safety and contamination control provisions.

9.2.7 Verification Reports

After each component, subsystem, payload, etc. verification activity has been completed, a report shall be submitted in accordance with the contract schedule (see DID 9-3 for guidance). For each analysis activity, the report shall describe the degree to which the objectives were accomplished, how well the mathematical model was validated by related test data, and other such significant

results. In addition, as-run verification procedures and all test and analysis data shall be retained for review.

9.2.8 System Performance Verification Report

At the conclusion of the verification program, a final system Performance Verification Report shall be delivered, comparing the hardware/software specifications with the final verified values (whether measured or computed). It is recommended that this report be subdivided by subsystem/instrument.

The System Performance Verification Report shall be developed and maintained "real-time" throughout the program. It will summarize the successful completion of verification activities, and showing that the applicable system performance specifications have been acceptably complied with prior to integration of hardware/software into the next higher level of assembly (see DID 9-3 for guidance).

10.0 WORKMANSHIP STANDARDS

10.1 GENERAL

The developer shall plan and implement a Workmanship Program to assure that all electronic packaging technologies, processes, and workmanship activities selected and applied meet mission objectives for quality and reliability. See Section 14 for additional information on ESD control.

10.2 APPLICABLE DOCUMENTS

The current status and/or any application notes for these standards can be can be found at http://workmanship.nasa.gov/. The most current version of these standards shall be used for new procurements. However, if a specific revision is listed for a referenced standard, only that revision is approved for use, unless otherwise approved by project management.

Conformal Coating and Staking:

NASA-STD-8739.1 "Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies"

Soldering:

Flight, Surface Mount Technology:

NASA-STD-8739.2 "Workmanship Standard for Surface Mount Technology"

Flight, Manual (hand):

NASA-STD-8739.3 "Soldered Electrical Connections"

Soldering Ground Systems:

IPC/ EIA J-STD-001C "Requirements for Soldered Electrical and Electronic Assemblies"

Electronic Assemblies – Ground Systems:

IPC-A-610 "Acceptability of Electronic Assemblies"

Crimping, Wiring, and Harnessing:

NASA-STD-8739.4 "Crimping, Interconnecting Cables, Harnesses, and Wiring"

Fiber Optics:

NASA-STD-8739.5 "Fiber Optic Terminations, Cable Assemblies, and Installation"

ESD Control:

ANSI/ESD S20.20	"Protection of Electrical and Electronic Parts, Assemblies and Equipment" (excluding electrically initiated explosive devices)

Printed Wiring Board (PWB) Design:

IPC-2221	"Generic Standard on Printed Board Design"
IPC-2222	"Sectional Design Standard for Rigid Organic Printed Boards"
IPC-2223	"Sectional Design Standard for Flexible Printed Boards"

PWB Manufacture:

IPC A-600	"Acceptability of Printed Boards"
IPC-6011	"Generic Performance Specification for Printed Boards"
IPC-6012	"Qualification and Performance Specification for Rigid Printed Boards" (Flight Applications supplemented with: GSFC/S312-P-003, "Procurement Specification for Rigid Printed Boards for Space Applications and Other High Reliability Uses")
IPC-6013	"Qualification and Performance Specification for Flexible Printed Boards"
IPC-6018	"Microwave End Product Board Inspection and Test"

10.3 DESIGN

10.3.1 Printed Wiring Boards

The PWB manufacturing and acceptance requirements identified in this chapter are based on using PWBs designed in accordance with the PWB design standards referenced above. Space flight PWB designs shall not include features that prevent the finished boards from complying with the Class 3 requirements of the appropriate manufacturing standard (e.g., specified plating thickness, internal annular ring dimensions, etc.).

Design of rigid PWBs shall not violate the requirements of the Association Connecting Electronics Industries (IPC) 6012B Performance Specification Sheet for Space and Military Avionics (PSSSMA). In the event of a conflict between the IPC design specifications, the 6012B Class 3 requirements, and the PSSSMA, the PSSSMA shall take precedence.

10.3.2 Assemblies

The design considerations listed in the NASA Workmanship and IPC standards listed above should be incorporated to the extent practical.

10.3.3 Ground Data Systems that Interface with Space Flight Hardware

Any portion of GDS assemblies (including GSE) that mate with flight hardware, that reside with space flight hardware in environments that simulate a space flight environment (e.g. connectors, test cables, etc.), or that interface directly with space flight hardware in any way, shall be designed and fabricated using space flight parts, materials and processes.

10.4 WORKMANSHIP REQUIREMENTS

10.4.1 Training and Certification

All personnel working on flight hardware shall be certified as having completed the required training appropriate to their involvement, as defined in the above standards or, when approved by project management, in the Developer's quality manual. This includes, but is not limited to, the aforementioned workmanship and ESD standards. At a minimum, certification shall include successful completion of formal training in the appropriate discipline. Recertification shall be in accordance with the requirements defined in the above workmanship standards.

10.4.2 Flight and Harsh Environment Ground Systems Workmanship

10.4.2.1 Printed Wiring Boards

PWBs shall be manufactured in accordance with Class 3 requirements in the above referenced IPC PWB manufacturing standards and the IPC 6012B PSSSMA. In the event of a conflict, the requirements specified in the IPC 6012B PSSSMA shall take precedence over all other specifications. The Developer shall provide PWB test coupons to the GSFC Materials Engineering Branch (MEB) or a GSFC/MEB approved laboratory for evaluation (see DID 10-1) per appropriate procurement specification. Coupon acceptance shall be obtained prior to population of flight PWBs. Test coupons and test reports are not required for delivery to GSFC/MEB if the Developer has the test coupons evaluated by a laboratory that has been approved by the GSFC/MEB, however, they shall be retained and included as part of the Project's documentation/data deliverables package.

10.4.2.2 Assemblies

Assemblies shall be fabricated using the appropriate workmanship standards listed above (i.e., NASA-STD-8739.3 for hand soldering; NASA-STD-8739.4 for crimping/cabling; NASA-STD-8739.5 for fiber optic termination and installation; NASA-STD-8739.2 for Surface Mount Soldering, etc.) and ANSI/ESD S20.20.

10.4.3 Ground Systems (Non-Flight) Workmanship

10.4.3.1 Printed Wiring Boards

Ground system PWBs not covered by Section 10.3.3 shall be manufactured in accordance with the Class 3 requirements in the above referenced IPC PWB manufacturing standards.

10.4.3.2 Assemblies

Assemblies shall be fabricated using the Class 3 requirements of J-STD-001, IPC-A-610, and ANSI/ESD S20.20. If any conflicts between J-STD-001 and IPC-A-610 are encountered, the requirements in J-STD-001 shall take precedence.

10.4.4 Documentation

The developer shall document the procedures and processes that will be used to implement the above referenced workmanship, design, and ESD control standards; including any procedures or process requirements referenced by those standards.

Alternate standards may be proposed by the developer. Proposals shall be accompanied by objective data documenting that mission safety or reliability will not be compromised. Their use is limited to the specific project and allowed only after they have been reviewed and approved by program management.

10.5 NEW AND ADVANCED MATERIALS AND PACKAGING TECHNOLOGIES

New and/or existing advanced materials and packaging technologies (e.g., multi-chip modules [MCMs], stacked memories, chip on board [COB], ball grid array [BGA], etc.) shall be reviewed and approved by the Parts Engineer for EEE parts or the Materials Assurance Engineer (MAE) for materials and processes.

10.6 HARDWARE HANDLING

The developer shall use proper safety, ESD control and cleanroom practices (where appropriate) when handling flight hardware. The electrostatic charge generation and contamination potential of materials, processes, and equipment (e.g., cleaning equipment, packaging materials, purging, tent enclosures, etc.) shall be addressed.

11.0 MATERIALS AND PROCESS REQUIREMENTS

11.1 GENERAL REQUIREMENTS

The LRO and its developers shall implement a Materials and Processes Control Plan (MPCP) to be implemented by the beginning of the hardware design stage (DID 11-1). The MPCP shall be compliant with the specific requirements of this section and the relevant LRO surveillance, documentation, safety and contamination control requirements specified in other sections of this MAR. The plan shall document developer's policies, procedures and guidelines for the selection, processing, inspection, testing, procurement and control of materials, and lubricants employed to meet the design and operational requirements of the LRO SC and their instruments. The LRO shall approve developer materials, lubrication usage, and associated manufacturing processes prior to their use in spaceflight hardware. The MPCP for activities at GSFC will be developed and implemented by the MAE assigned to the LRO from the MEB.

Existing developer in-house documentation equivalent to DID 11-1 may be used and referenced in the plan to address how these requirements are to be met, and shall be submitted to the LRO for approval. All appropriate sub-developers shall participate in the MPCP to the extent required by the prime developer and the LRO in order to meet these requirements. The plan shall address how the developer will ensure the flow down of applicable MPCP requirements to sub-developers. The MPCP may be incorporated in the developer's Performance Assurance Implementation Plan.

11.2 MATERIALS SELECTION REQUIREMENTS

To qualify as a material compliant with intended spaceflight use, a material must have a satisfactory flight heritage, be approved by the LRO and meet the following applicable selection criteria as defined herein for:

1. Vacuum outgassing
2. Stress corrosion cracking (SCC)
3. Lubrication requirements
4. Manufacturing process selection
5. Fastener integrity

The selection and use of material with hazardous properties (such as flammability and toxicity) shall meet the requirements specified in AFSCM91-710 Range Safety User Requirements Manual, Chapters 10 and 12.

A material that has limited spaceflight heritage or does not meet the applicable selection requirements listed above shall be considered non-compliant. In that case, if there are no alternatives available to select a compliant material, the material's usage will be justified and approved prior to use for the desired application on the basis of test, similarity, analyses, inspection, existing data, or a combination of those data. . Materials used in structural applications shall be highly resistant to SCC as specified in MSFC-STD-3029. A Materials

Usage Agreement (MUA) (Figure 11-1) and/or a Stress Corrosion Evaluation Form (Figure 11-2) shall be submitted to the LRO for approval for use of the proposed non-compliant material (DID 11-3 & 11-4). Both forms will be required for a material that does not meet the SCC requirements. The Developer may use their own forms if they contain equivalent information and justification.

<table>
<tr><td colspan="3">MATERIAL USAGE AGREEMENT</td><td colspan="3">USAGE AGREEMENT NO.:</td><td>PAGE OF</td></tr>
<tr><td>PROJECT:</td><td colspan="2">SUBSYSTEM:</td><td colspan="3">ORIGINATOR:</td><td>ORGANIZATION:</td></tr>
<tr><td>DETAIL DRAWING</td><td colspan="2">NOMENCLATURE</td><td colspan="2">USING ASSEMBLY</td><td colspan="2">NOMENCLATURE</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="3">MATERIAL & SPECIFICATION</td><td colspan="4">MANUFACTURER & TRADE NAME</td></tr>
<tr><td colspan="3"></td><td colspan="4"></td></tr>
<tr><td>USAGE</td><td>THICKNESS</td><td>WEIGHT</td><td>EXPOSED AREA</td><td colspan="3">ENVIRONMENT</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td>PRESSURE</td><td>TEMPERATURE</td><td>MEDIA</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="7">APPLICATION:</td></tr>
<tr><td colspan="7">RATIONALE:</td></tr>
<tr><td colspan="3">ORIGINATOR:</td><td colspan="2">PROJECT MANAGER:</td><td colspan="2">DATE:</td></tr>
</table>

Figure 11-1. Material Usage Agreement

1. Part Number _____
2. Part Name _____
3. Next Assembly Number _____
4. Manufacturer _____
5. Material _____
6. Heat Treatment _____
7. Size and Form _____
8. Sustained Tensile Stresses-Magnitude and Direction

a. Process Residual _____
b. Assembly _____
c. Design, Static _____

9. Special Processing _____
10. Weldments

a. Alloy Form, Temper of Parent Metal _____
b. Filler Alloy, if none, indicate _____
c. Welding Process _____
d. Weld Bead Removed - Yes ( ), No ( ) _____
e. Post-Weld Thermal Treatment _____
f. Post-Weld Stress Relief _____

11. Environment _____
12. Protective Finish _____
13. Function of Part _____
14. Effect of Failure _____
15. Evaluation of Stress Corrosion Susceptibility _____
16. Remarks: _____

Figure 11-2. Stress Corrosion Evaluation Form

The LRO and its developers shall create and maintain an As-Designed Materials and Processes List (ADMPL) of all materials planned for use in the configured flight hardware (DID 11-2). The initial ADMPL and subsequent updates shall be submitted to the LRO and LRO MAE for review and approval (DID 11-2). An As-Built Materials List (ABML) shall also be prepared and submitted to the LRO for review and approval. The ABML is generally the final ADMPL that includes all materials, processes, and lubrication being used in the as-built configured flight article designated to fly and as delivered on-orbit.

Each materials list shall be an itemization of the materials, processes and lubricants used in the configured flight article and shall contain as a minimum the information in Figures 11-3 through 11-6, respectively.

In order to minimize materials and lubricant problems during use in space hardware, the developers shall anticipate and consider potential application problem areas during the material selection process. Potential problem areas and application factors to be considered include radiation effects, electrostatic discharging, thermal cycling, SCC, galvanic corrosion, hydrogen embrittlement, lubrication, contamination of cooled surfaces, composite materials, atomic oxygen , limited life, vacuum outgassing, toxicity, flammability and fracture toughness, as well as the properties required by each material usage or application.

11.2.1 Inorganic Materials

The developer shall prepare and document an Inorganic Materials List (Figure 11-3) or the Developer's equivalent (DID 11-7). The list shall be submitted to the MAE for review and approval.

GSFC Spacecraft Inorganic Materials List

Spacecraft		System/Experiment	
Contractor		Contractor Address	
Prepared by		Phone and Fax #	
GSFC MAE		Date Prepared	
Date Rec'd		Project SAM	

Item No.	Material Identification	Condition	Application	Expected Environment	MSFC-STD-3029 Rating

Figure 11-3. Inorganic Materials List

The use of tin, zinc, and cadmium platings in any flight application requires an MUA prior to use of that material. Bright tin, cadmium, and zinc platings have the potential for developing whisker growths. For tin, these have been measured up to 12.5 microns in diameter and up to 10 millimeters (mm) in length. These whiskers can result in short circuits, plasma arcing, and debris

generation within the SC. Zinc and cadmium platings also evaporate in vacuum environments and may redeposit on optics or electronics, posing potential risks to flight hardware.

11.2.2 Vacuum Outgassing of Polymeric Materials

Only materials that have a total mass loss (TML) less than 1.00% and a collected volatile condensable mass (CVCM) less than 0.10% shall be approved for use in a vacuum environment. Material vacuum outgassing shall be determined in accordance with American Society for Testing of Materials (ASTM) E-595. If a material exceeds these maximum limits, the developers shall be required to either replace with a compliant material or bring it into compliance via a vacuum bakeout, or to submit a MUA for its usage. In general, a material is qualified on a product-by-product basis. However, lot testing may be required of any material for which lot variation is evident or suspected. In such cases unless supporting justification is provided negating additional lot testing via an MUA, material approval is contingent upon lot testing.

The LRO and its developers shall prepare and submit a Polymeric Materials List as indicated in Figure 11-4 (DID 11-5).

GSFC Spacecraft Polymeric Materials List

Spacecraft _____ System/Experiment _____ Date Prepared _____

Contractor _____ Contractor Address _____ Phone & Fax # _____

Prepared by _____

GSFC MAE _____

Project SAM _____

Date Rec'd _____

Amount Code		
Area, cm^2	Vol, cc	wt, gm
1. 0-1	A. 0-1	a. 0-1
2. 2-100	B. 2-50	b. 2-50
3. 101-1000	C. 51-500	c. 51-500
4. > 1000	D. > 500	d. > 500

Item No.	Component	Material Identification	Mix Formula	Cure Details	Amount Code	Expected Environment	ASTM-E-595 %TML	ASTM-E-595 %CVCM

Figure 11-4. Polymeric Materials List

11.2.3 Lubrication Systems

Lubricants shall be selected for use with materials on the basis of flight heritage and valid test results that confirm the suitability of the composition and the performance characteristics for each specific application, including compatibility with the anticipated environment and contamination concerns.

All lubricated mechanisms shall be life tested unless it can be established and documented that a valid flight heritage exists to an identical mechanism used in an identical flight application or to an identical mechanism that has been separately qualified by suitable life testing (DID 11-10).

The LRO and its developers shall prepare and submit a Lubrication Materials List as indicated in Figure 11-5 (DID 11-9). In addition, the developer may be requested to submit supporting applications data.

GSFC Spacecraft Lubrication Materials List

Spacecraft		System/Experiment	
Contractor		Contractor Address	
Prepared by		Phone and Fax #	
GSFC MAE		Date Prepared	
Date Rec'd		Project SAM	

Wear Codes

Type	# Cycles	Speed
CUR continuous unidirectional rotation	A 1-10^2	rpm rev/min
CO continuous oscillation	B 10^2-10^4	opm osc/min
IR intermittent rotation	C 10^4-10^6	vs variable
IO intermittent oscillation	D >10^6	cpm cm/min
SO small oscillation (<30)		
LO large oscillation (>30)		
CS continuous sliding		

Item No.	Component Type, Size, and Material	Proposed Lubricant and Amount	Type and # of Wear Cycles	Speed, Temp, & Atm of Operation	Type of Loads and Amount

Figure 11-5. Lubrication Materials List

11.2.4 Process Selection Requirements

Manufacturing processes (e.g., conformal coating, adhesive bonding, lubrication, heat treatment, welding, chemical or metallic coatings, etc.) shall be carefully selected to preclude unacceptable material property changes during exposure to flight environments that could cause adverse effects to the material and/or to the intended applications.

The LRO and its developers shall create and maintain a Materials Processes List with the format and content indicated in Figure 11-6 (DID 11-11).

GSFC Spacecraft Materials Processes List

Spacecraft		System/Experiment	
Contractor		Contractor Address	
Prepared by		Phone and Fax #	
GSFC MAE		Date Prepared	
Date Rec'd		Project SAM	

Item No.	Process Type	Contractor Spec #	MIL, ASTM or other Spec #	Description of Material Processed	Spacecraft Application

Figure 11-6. Materials Processes List

11.2.5 Fasteners

The LRO and its developers shall comply with the procurement and test requirements for flight hardware and critical GSE fasteners contained in 541-PG-8072.1.2, Goddard Space Flight Center Fastener Integrity Requirements. The LRO and its developers shall implement a Fastener Control Plan (DID 11-8) to comply with the requirements outlined in 541-PG-8072.1.2.

Fasteners made of plain carbon or low alloy steel shall be protected from corrosion. When plating is specified, it shall be compatible with the space environment. On steels harder than RC 33, a plating process that does not embrittle the steel shall be utilized.

11.3 MATERIALS USED IN "OFF-THE-SHELF-HARDWARE"

"Off-the-shelf hardware" for which a detailed materials list is not available and where the included materials cannot be easily identified and/or replaced shall be treated as non-compliant. The LRO and its developers shall submit a MUA that defines the appropriate measures that will be used to ensure that all materials in the "off-the-shelf" hardware are acceptable for use. It may be possible to replace unknown or non-compliant materials within the hardware with compliant materials, or hermetically seal, or vacuum bake out the questionable hardware to bring the hardware into a suitable condition for use. Such approaches shall be documented in the MUA. When a vacuum bake-out is the selected method, it shall incorporate a quartz crystal microbalance (QCM) and cold finger to enable a determination of the duration and effectiveness of the bake-out as well as compliance with the project contamination plan and error budget.

11.4 MATERIALS PROCUREMENT REQUIREMENTS

Raw materials purchased by the LRO and its developers shall be accompanied by a Certificate of Raw Materials Compliance (DID 11-12) and, where applicable, the results of nondestructive, chemical and physical tests. When requested, this information shall be made available to the LRO for review.

11.4.1 Incoming Inspection Requirements

Each developer shall perform, or be responsible for the performance of applicable incoming tests and inspections of materials to ensure that they meet the requirements of the procurement specification. Unless previously accomplished and accepted by government or developer field personnel, incoming testing and inspections shall be performed upon receipt of the parts or materials. The inspection and testing of materials shall be conducted in accordance with a plan approved by the MAE.

11.5 SHELF-LIFE-CONTROL REQUIREMENTS FOR POLYMERIC MATERIALS

Polymeric materials that have a limited shelf life shall be controlled by a process that identifies the start date (manufacturing date, shipment date, or date of receipt, etc.), the storage conditions associated with a specified shelf life, and expiration date. Materials such as o-rings, rubber seals, tape, uncured polymers, lubricated bearings and paints shall be included. When a limited-life

piece part is installed in a subassembly, the subassembly item shall be included in the Limited-Life Items List. (DID 4-9)

Materials usage beyond the expiration date requires that the developer demonstrate by means of appropriate testing that the material's properties are not compromised for the intended use. In these situations, a waiver (DID 11-6) shall be written and submitted to the LRO for approval prior to use of the material beyond the expiration date.

11.6 FAILURE ANALYSIS

Failure analysis shall be performed on part and material failures experienced during assembly and testing. Failures shall be analyzed to the extent necessary to understand the failure mode and cause, to detect and correct out-of-control processes, to determine the necessary corrective actions, and to determine lot disposition. When required, a failure analysis report shall be prepared and documented. The MAE shall determine and implement appropriate corrective action for each material and processes (M&P) failure. All failures, and the results of final failure analysis, shall be documented.

Failure analysis reports shall be retrievable for the duration of the contract, and shall be available to GSFC.

11.7 PRESERVATION AND PACKING

Preservation, packaging, and packing shall be in accordance with the item and the system requirements. All parts that are subject to degradation by ESD shall be packaged in accordance with the approved ESD procedures.

11.8 HANDLING

Handling (including storage) procedures shall be instituted to prevent part and material degradation. The handling procedures shall be retained through inspection, kitting, and assembly and shall be identified on "build to" documentation. The following criteria shall be used as a minimum for establishing handling and storage procedures for parts and materials:

a. Control of environment, such as temperature, humidity, contamination, and pressure.

b. Measures and facilities to segregate and protect parts and materials routed to different locations, such as to the materials review crib, to a laboratory for inspection, or returned to the manufacturer from unaccepted shipments.

c. Space quality parts shall be stored in easily identified containers.

d. Control measures to limit personnel access to parts and materials during receiving inspection and storage.

e. Facilities for interim storage of parts and materials.

f. Provisions for protective cushioning, as required, on storage area shelves, and in storage and transportation containers.

g. Protective features of transportation equipment design to prevent packages from being dropped or dislodged in transit.

h. Protective bench surfaces on which parts and materials are handled during operations such as test, assembly, inspection, and organizing kits.

i. Required use of gloves, finger cots, tweezers, or other means when handling parts to protect the parts from contact by bare hands.

j. Provisions for protection of parts susceptible to damage by ESD.

k. Unique parts and materials criteria.

11.9 DATA RETENTION

The program shall maintain records of incoming inspection tests, lot qualification and acceptance test data, radiation hardness assurance test data, traceability data and other data as determined by the MAE for a period of time specified by GSFC.

12.0 EEE PARTS CONTROL PROGRAM SUPPORT

12.1 GENERAL

Each developer, contractor and subcontractor (hereon referred to as "the Developer") shall plan and implement an EEE Parts Control Program to assure that all parts selected for use in flight hardware meet mission objectives for quality and reliability. The program shall be in place to effectively support the design and selection processes for the duration of the contract. The Developer shall control the selection, application, evaluation, and acceptance of all parts through a Parts Control Board (PCB), or equivalent developer documented process of parts control and shall be approved by GSFC.

All parts shall be selected and processed in accordance with GSFC EEE-INST-002, "EEE Parts Selection, Screening Qualification and Derating," for part quality level 2. Exceptions for use of a lesser grade part with additional testing shall be made on a case by case basis only when a level 2 part is not available. Such exceptions require approval by the PCB.

The Developer shall prepare a Parts Control Plan (PCP) (see DID 12-1) describing the approach and methodology for implementing their Parts Control Program. The PCP shall also define the Developer's criteria for parts selection and approval based on the guidelines of this section. The Developer Project Parts Engineer (PPE) may work with the GSFC PPE to assure that all necessary information is contained in the PCP.

Each developer shall designate one key individual as the PPE, who shall have the prime responsibility for management of the EEE Parts Control Program. This individual shall have direct, independent and unimpeded access to the GSFC PPE and PCB. The PPE shall work with design engineers, radiation engineers, reliability engineers and the GSFC PPE to perform part selection and control.

12.2 PARTS CONTROL BOARD

The developer shall establish a PCB or similar documented system to facilitate the management, selection, standardization, and control of parts and associated documentation for the duration of the contract. The PCB shall be responsible for the review and approval of all EEE parts, for conformance to established criteria as defined herein (including radiation effects), and for developing and maintaining a Project-Approved Parts List (PAPL). In addition, the PCB is responsible for providing assistance in all parts activities, such as part failure investigations, disposition of part non-conformances, and part problem resolutions. PCB operating procedures shall be included as part of the PCP.

12.2.1 PCB Responsibilities

The responsibilities of the PCB shall include, but not be limited to, the following:

- Evaluate EEE parts for conformance to established criteria and inclusion in the parts list.
- Develop and maintain a PAPL.
- Review and approve EEE part derating as necessary for unique applications.
- Define testing requirements.
- Review unique applications (including radiation effects).
- Track part failure investigations and non-conformances.

12.2.2 PCB Meetings, Notification, and Reports

PCB meetings shall be convened on a regular basis, or as needed. The PCB meeting may be conducted via phone conversation, as needed on a case by case basis. The GSFC PPE shall be a permanent voting member of PCB meetings. The developer PPE shall prepare PCB reports to document all decisions made, with a copy provided to GSFC within five days of the meeting (DID 12-2). GSFC will retain the right to overturn decisions involving non-conformances within ten days of receipt of the meeting minutes.

The Developer PPE shall notify attendees at least five working days in advance of all upcoming meetings except in an emergency situation. Notification shall, at a minimum, include a proposed agenda and Parts Identification List (PIL) of candidate parts.

12.2.3 PCB Membership

At a minimum, the PCB membership shall consist of the developer's Product Assurance Manager, developer PPE, GSFC PPE, and GSFC Project Radiation Engineer (PRE) (GSFC Code 561) when required. The developer PPE and GSFC PPE shall participate in all PCB meetings. The GSFC System Assurance Manager (SAM), or designee, may attend as necessary. The developer PPE, GSFC PPE and GSFC PRE shall be permanent working and voting members of the PCB. The developer PPE shall assure that the appropriate individuals with engineering knowledge and skills are represented as necessary at meetings, such as part commodity specialists, radiation engineers, or the appropriate subsystem design engineer.

If there are any parts issues that cannot be resolved at the PCB level, the issues shall be elevated to the GSFC (LRO) Program Manager for disposition.

12.3 PART SELECTION AND PROCESSING

All part commodities identified in EEE-INST-002 are considered EEE parts and shall be subjected to the requirements set forth in this section. EEE parts types that do not fall into any of

the categories covered in EEE-INST-002 shall be reviewed on a case by case basis using the closest NASA, Defense Supply Center Columbus (DSCC), or government controlled specification. In the event a suitable government baseline specification does not exist, the developer PPE shall consult the GSFC PPE to identify the best available industry standard for that particular commodity, and develop appropriate procurement, screening and qualification specifications.

12.3.1 Parts Selection

Parts shall be selected from the GSFC EEE-INST-002, "Parts Selection, Screening, Qualification and Derating" document, or the NASA Parts Selection List (NPSL) for quality level 2 or better. Exceptions for use of a lower grade shall only be made on a case by case basis when a level 2 part is unavailable. Such exceptions require approval by PCB. The use of a lower grade part requires additional testing be performed in accordance with EEE-INST-002 to upgrade the part to level 2.

EEE-INST-002 contains value added testing for a number of parts listed in the NPSL. These tests include Particle Impact Noise Detection (PIND) testing for all EEE devices, surge current testing for tantalum capacitors and dielectric screening for several types of ceramic capacitors. These, and any other value added tests listed in EEE-INST-002, shall be performed to enhance the reliability of parts. PCB approval is required if there is any deviation from any screening or qualification tests as specified in EEE-INST-002.

12.3.2 Radiation Requirements for Parts Selection

All parts shall be selected to perform nominally in the predicted radiation environment, including the applicable Radiation Design Margin (RDM). The radiation environment causes the following three main degradation effects, which must be accounted for in all active parts selection:

- Total Ionizing Dose (TID) (including Enhanced Low Dose Rate [ELDR] effects) – Parts shall be selected to ensure adequate performance in the application, up to a dose of twice the expected mission dose. Linear bipolar parts shall be assumed to be ELDR susceptible, unless the parts have been successfully tested and shown insensitive.

- Single-Event Effects (SEE) – Parts must be assessed for the potential of Single-Event Upset (SEU) or Single-Event Transient (SET), which requires analysis of the circuit application on a case by case basis. Parts susceptible to Single-Event Latch-up (SEL) should be avoided. If performance demands the use of an SEL susceptible part, measures shall be implemented to ensure that SEL induced damages (both prompt and latent) are mitigated and that SC performance is not compromised. These measures must be approved by the GSFC PRE and PPE before the part can be added to the PAPL. Applied voltages for power Metal-Oxide-Semiconductor Field Effect Transistors (MOSFETs), Field Effect Transistors (FETS), and bipolar junction transistors shall be in the safe operating ranges for these devices, based on Single-Event Gate Rupture (SEGR)/Single-Event Burn-out (SEB) test data.

- Displacement Damage – Parts shall be able to withstand the displacement damage to high energy protons, to twice the fluence expected in the predicted LRO environment. This effect can cause significant damage in optical devices.

These effects and others may require individual part application analysis to be performed as necessary by the PRE. The developer shall document the radiation analysis of each part as applicable.

12.3.3 Custom or Advanced Technology Devices

Devices such as custom hybrid microcircuits, detectors, Application Specific Integrated Circuits (ASICs), and MCMs shall also be subject to parts control and include a design review appropriate for the individual technology. The design review will include element evaluation to assure each element's reliability (review should include such items as burn-in, voltage conditioning, sample size, element derating, etc.), device construction and assembly process (including materials evaluation for such items as contamination concerns, metal whisker concerns, and adequate material thermal matching; materials specialists may be consulted as necessary). A customer source inspection may be required.

A procurement specification may be required for parts in this category based on the recommendation of the PPE. These specifications shall fully describe the item being procured, and shall include physical, mechanical, environmental, electrical test requirements, and QA provisions necessary to control manufacture and acceptance. Screening requirements designated for the part may be included in the procurement specification. Test conditions, burn-in circuits, failure criteria, and lot rejection criteria will be included. For lot acceptance or rejection, the Percentage of Defectives Allowable (PDA) in a screened lot shall be in accordance with that prescribed in the closes military part specification.

12.3.4 Plastic Encapsulated Microcircuits

The use of Plastic Encapsulated Microcircuits (PEMs) and plastic semiconductors is discouraged, however, when use of PEMs is necessary to achieve unique performance requirements unachievable using hermetic high reliability microcircuits, plastic encapsulated parts must meet the requirements of EEE-INST-002. The PCB shall review the procurement specification, application of part, and storage processes for PEMs, to assure that all aspects of EEE-INST-002 have been met.

12.3.5 Verification Testing

Re-performance of screening tests, which were performed by the manufacturer or authorized test house, as required by the military or procurement specification, is not required unless deemed necessary by failure history, GIDEP Alerts, age, or other reliability concerns. If required, testing shall be performed in accordance with GSFC EEE-INST-002, or as determined by the PCB.

12.3.6 Parts Approved on Prior Programs

Parts previously approved by GSFC for other projects via prior PCB activity or a Nonstandard Parts Approval Request (NSPAR) shall not be granted "grandfather approval" on LRO. However, existing approval packages may be brought to the PCB as an aid to present candidate parts for approval. (Preparation of NSPARs is not a requirement for LRO.)

12.4 PART ANALYSIS

12.4.1 Destructive Physical Analysis

A sample of each lot date code of microcircuits, hybrid microcircuits, and semiconductor devices may be subjected to a Destructive Physical Analysis (DPA) based on PCB recommendation. All other parts may require a sample DPA if it is deemed necessary as indicated by failure history, GIDEP Alerts, or other reliability concerns. DPA tests, procedures, sample size and criteria shall be as specified in GSFC specification S-311-M-70, "Destructive Physical Analysis." Contractor's procedures for DPA may be used in place of S-311-M-70 and shall be submitted with the PCP for concurrence prior to use. The PCB shall consider variation to the DPA sample size requirements, due to part complexity, availability or cost on a case by case basis.

12.4.2 Failed EEE Parts

An EEE part failure is defined as a failure for which the part itself is the intrinsic cause, which occurs while the part is operating within its specification limits. Emphasis shall be placed on detection, analysis, and feedback of failure data during unit level testing. The developer shall have a method in place to report all EEE component failures. Failures occurring during EEE part screening and qualification shall be reported. In addition, failures that occur after the first application of power at the subassembly level (and continuing through unit, subsystem and system levels) during qualification and acceptance testing of flight hardware shall be reported. The failure reporting plan shall include identification of failed parts, notification within an approved time of failure, retrieval of failed/overstressed parts, part failure analysis, and documentation of all pertinent information related to each failure. The failure reporting plan shall be documented and presented to the PCB and the GSFC Project Office for review and approval.

12.4.3 Failure Analysis

When a component part Failure Analysis (FA) is necessary to support a Failure Review Board (FRB), the developer shall prepare a part Failure Analysis Report. The contractor PPE shall submit the completed report to the PCB for review and approval in order to assure proper documentation is presented for the FRB. The failure report form shall provide the following information at a minimum:

- The failed part's identity (part name, part number, reference designator, manufacturer, manufacturing lot/date code, and part serial number if applicable), and symptoms by which the failure was identified (the conditions observed as opposed to those expected).

- The name of the unit or subsystem on which the failure occurred, date of failure, the test phase, and the environment in which the test was being conducted.

- An indication of whether the failure of the part or item in question constitutes a primary or secondary (collateral) failure (caused by another failure in the circuit and not a failure on its own merit).

The completed failure report shall include copies of any supporting photographs, X-rays, metallurgical data, microprobe or spectrographic data, Scanning Electronic Microscope (SEM) photographs, pertinent variables (electrical and radiation) data, etc. Radiation data shall be submitted where it is deemed relative to the failure mechanism.

12.5 ADDITIONAL REQUIREMENTS

12.5.1 Parts Age Control

All active EEE parts procured with date codes indicating that more than five years have elapsed from the date of manufacture to date of procurement shall be subjected to a re-screen (and sample DPA per PCB recommendation). Parts taken from user inventory older than five years do not require re-screen, provided they have been properly stored (refer to Section 14). Proper storage means maintaining the parts within their rated temperature range in an area protected from conditions that create electrostatic damage or contaminants that may affect their functionality (e.g. corrosive atmospheres that damage the plating on the leads or terminations). Storage areas shall be inspected and electrostatic discharge (ESD) certified for proper equipment and handling procedures in accordance with ANSI/EDS-S20.20, "Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices)."

An alternate contractor method of controlling parts age may be used upon review and approval by the PCB.

Parts over ten years from the date of manufacture to date of procurement are discouraged. Exceptions shall be reviewed on a case by case basis and require approval of the PCB. Parts stored in uncontrolled conditions where they may be exposed to ESD, the elements, or sources of contamination shall not be used.

12.5.2 Derating

All EEE parts shall be used in accordance with the derating guidelines of GSFC EEE-INST-002. The developer's derating policy may be used in place of the GSFC guidelines and shall be submitted with the developer PCP for approval. The developer shall maintain documentation on parts derating analysis and make it available for GSFC review.

12.5.3 Alerts

The developer shall be responsible for the review and disposition of all GIDEP Alerts on parts proposed for flight use. In addition, any NASA Alerts and Advisories provided to the developer by GSFC shall be reviewed and dispositioned. Alert applicability, impact, and corrective actions shall be continuously documented and reported to GSFC. (See DID 12-4) The review process shall continue from delivery to launch.

12.5.4 Prohibited Metals

Pure tin plating shall not be used in the construction and surface finish of EEE parts proposed for space hardware. Only alloys containing less than 97% tin are acceptable.

The use of pure cadmium or zinc is prohibited in the construction and surface finish of space hardware. All cadmium alloys or zinc alloys (e.g. brass) must be completely over plated with an approved metal. The GSFC Materials Branch shall be consulted as necessary.

12.6 PARTS LIST

The developer shall document and maintain a PAPL and a PIL for the duration of the project. The contractor shall submit the PAPL to GSFC. Parts must be approved for listing on the PAPL before initiation of procurement activity. All submissions to the LRO Project shall include a computer compatible form (Microsoft Excel, Microsoft Access, etc.; consult GSFC PPE for acceptable format).

12.6.1 Parts Identification List

The PIL shall be a real time working list of all parts proposed for use in flight hardware. The PIL is prepared from design team inputs or subcontractor inputs, and is used for presenting and tracking candidate parts to the PCB. The PIL shall include the following information at a minimum: part number, part name or description, manufacturer, manufacturer's generic part number, drawing number, specifications, comments as necessary (to indicate problems, long lead times, additional testing imposed, application unique notes, etc). The PIL shall also have radiation effects information on active devices such as semiconductors, microcircuits and optoelectronic parts. (See DID 12-3)

12.6.2 Program Approved Parts List

The PAPL shall be the only listing of approved parts for flight hardware, and shall be the combined listing of all parts submitted through PILs that are approved by the PCB, plus approval status and disposition notes. Only parts that have been evaluated and approved by the PCB shall be listed in the PAPL. The PCB shall assure standardization of parts listed in the PIL across various systems and subsystems. (See DID 12-3)

12.6.3 As-Built Parts List

An As-Built Parts List (ABPL) shall also be prepared and submitted to the LRO by the Contractor PPE. The ABPL is generally a final compilation of all parts as installed in flight equipment, with additional "as-installed" part information such as manufacturer name, Commercial and Government Entity (CAGE) code, Lot-Date code, part serial number (if applicable), box identification and/or part location. Provisions shall be in place to find quantity used and provide traceability to box or board location through build paperwork. The manufacturer's plant specific CAGE code is preferred, but if unknown, the supplier's general CAGE code is sufficient. (See DID 12-3)

12.7 DATA REQUIREMENTS

Attributes summary data shall be kept available to GSFC for all testing performed. Variable data (read and record) shall be recorded for initial, interim and final electrical test points and shall be kept available to GSFC.

For flight lots with samples subjected to Radiation Lot Acceptance Test (RLAT), the radiation report that identifies parameter degradation behavior shall be provided to the PCB, and variables data acquired during radiation testing shall be kept available to GSFC.

12.7.1 Radiation Hardness

All developers shall have a method in place for retention of data generated for parts tested and used in flight hardware. The data shall be kept on file in order to facilitate future risk assessment and technical evaluation. In addition, the developer shall retain all part functional failures, all destructive and non-flight non-destructive test samples, which could be used for future validation of parts for performance under certain conditions not previously accounted for. These devices shall be kept until launch. PIND test failures may be submitted for DPA or radiation testing, but are not recommended for use in engineering models. Data shall be retained for the useful life of the SC, unless otherwise permitted by PCB.

All historical records and data required to support these records shall be retained for a period of five years and shall be provided to GSFC on request.

13.0 CONTAMINATION CONTROL REQUIREMENTS

13.1 GENERAL

The developer shall plan and implement a contamination control program appropriate for the hardware. The program shall establish the specific cleanliness requirements and delineate the approaches to be followed in a Contamination Control Plan (CCP) (see DID 13-1).

Contamination includes all materials of molecular and particulate nature whose presence degrades hardware performance. The source of the contaminant materials may be the hardware itself, the test facilities, and the environments to which the hardware is exposed.

13.2 CONTAMINATION CONTROL VERIFICATION PROCESS

The developer shall develop a contamination control verification process. The verification process shall be performed in order:

a. Determination of contamination sensitivity.

b. Determination of a contamination allowance.

c. Determination of a contamination budget.

d. Development and implementation of a contamination control plan.

Each of the above activities shall be documented and submitted to GSFC for concurrence/approval.

13.3 CONTAMINATION CONTROL PLAN

The developer shall prepare a CCP that describes the procedures that will be followed to control contamination. It shall establish the implementation and describe the methods that will be used to measure and maintain the levels of cleanliness required during each of the various phases of the item's lifetime. In general, all mission hardware should be compatible with the most contamination-sensitive components.

13.4 MATERIAL OUTGASSING

In accordance with ASTM E595, NASA RP 1124 shall be used as a guide. Individual material outgassing data shall be established based on each component's operating conditions. Established material outgassing data shall be verified and shall be reviewed by GSFC.

13.5 THERMAL VACUUM BAKEOUT

The developer shall perform thermal vacuum bakeouts of all hardware. The parameters of such bakeouts (e.g., temperature, duration, outgassing requirements, and pressure) must be individualized depending on materials used, the fabrication environment, and the established

contamination allowance. Thermal vacuum bakeout results shall be verified and shall be reviewed by GSFC.

13.6 HARDWARE HANDLING

The developer shall practice cleanroom standards in handling hardware. The contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, bagging (e.g., anti-static film materials), and purging shall be described in detail for each subsystem or component at each phase of assembly, integration, test, and launch.

14.0 ELECTROSTATIC DISCHARGE CONTROL

14.1 GENERAL

The developer shall document and implement an ESD Control Program to assure that all manufacturing, inspection, testing, and other processes will not compromise mission objectives for quality and reliability due to ESD events. (See DID 14-1)

14.2 APPLICABLE DOCUMENTS

The current status and/or any application notes for these standards can be obtained at http://workmanship.nasa.gov. The most current version of these standards should be used for new procurements. Included shall be ANSI/ESD S20.20, "ESD Association Standard for the Development of an Electrostatic Discharge Control Program for protection of electrical and electronic parts, assemblies, and equipment (excluding electrically initiated explosive devices)."

However, if a specific revision is listed for a referenced standard, only that revision is approved for use unless otherwise approved by project management.

14.3 ELECTROSTATIC DISCHARGE CONTROL REQUIREMENTS

The developer shall document and implement an ESD Control Program in accordance with ANSI/ESD S20.20, "Protection of Electrical and Electronic Parts, Assemblies and Equipment (excluding electrically initiated explosive devices)," suitable to protect the most sensitive component involved in the project. At a minimum, the ESD Control Program shall address training, protected work area procedures and verification schedules, packaging, facility maintenance, storage, and shipping.

All personnel who manufacture, inspect, test, otherwise process electronic hardware, or require unescorted access into ESD protected areas shall be certified as having completed the required training, appropriate to their involvement, as defined in ANSI/ESD S20.20 or in the developer's quality manual prior to handling any electronic hardware.

Electronic hardware shall be manufactured, inspected, tested, or otherwise processed only at designated ESD protective work areas. These work areas shall be verified on a regular schedule as identified in the developer's ESD Control Program; an ESD Control Program that has been approved by the procuring organization.

Electronic hardware shall be properly packaged in ESD protective packaging at all times when not actively being manufactured, inspected, tested, or otherwise processed.

Alternate standards may be proposed by the developer. Their use is limited to the specific project and is allowed only after they have been reviewed and approved by the GSFC Project Office.

Materials selected for packaging or protecting ESD sensitive devices shall not leach chemicals, leave residues, or otherwise contaminate parts or assemblies (e.g., "pink poly" is well known for its outgassing of contaminants and should only be used for storing documentation or other non-hardware uses).

15.0 GIDEP ALERTS AND PROBLEM ADVISORIES

15.1 GENERAL

The developer shall participate in the GIDEP in accordance with the requirements of the GIDEP SO300-BT-PRO-010 ("GIDEP Operations Manual") and SO300-BU-GYD-010 ("Government-Industry Data Exchange Program Requirements Guide"), available from the GIDEP Operations Center, Post Office (PO) Box 8000, Corona, California 92878-8000.

The developer shall review all GIDEP Alerts, GIDEP Safe-Alerts, GIDEP Problem Advisories, GIDEP Agency Action Notices, NASA Advisories and any informally documented component issues presented by Code 303, to determine if they affect the developer products produced for NASA. For the above mentioned alerts and advisories that are determined to affect the program, the developer shall take action to eliminate or mitigate any negative effect to an acceptable level.

The developer shall provide a matrix that shows whether or not GIDEPs and related alerts impact their hardware and this matrix shall be maintained and updated as new alerts are issued or new hardware is received. It is the developers' responsibility to review and update this matrix during the life of the project.

The developer shall generate the appropriate failure experience data report(s) (GIDEP Alert, GIDEP Safe-Alert, GIDEP Problem Advisory) on a monthly basis, in accordance with the requirements of GIDEP SO300-BT-PRO-010 and SO300-BU-GYD-010 whenever failed or nonconforming items, available to other buyers, are discovered during the course of the contract.

16.0 END ITEM DATA PACKAGE

The developer shall prepare an end item data package (EIDP) which documents the design, fabrication, assembly and test of the hardware and software being delivered for integration. The following list details what shall be contained in the EIDP at a minimum. (DID 16-1) The EIDP shall be submitted for review and approval by GSFC at the PSR.

Acceptance testing (as run) procedures and reports including total number of failure free testing

Environmental Testing (as run) reports

Final Assembly Work Order

Material Certification or Analysis Forms

Waivers, Deviations or MUAs

As-built EEE parts list

As-built materials list (ABML)

End Item Inspection Report

Nonconformance or problem/failure reports and corrective action summaries

List of Open items or one time occurrences

As-built final assembly drawing

Any pertinent analyses (mechanical, electrical, reliability, stress, thermal, worst case)

As-built configuration list (Item, Manufacturer, Model, etc)

Certificate of Compliance signed by management

17.0 APPLICABLE DOCUMENTS LIST

DOCUMENT	DOCUMENT TITLE
AFSCM 91-710	Range Safety Users Requirements Manual
ANSI/ASQC Q9000-3	Quality Management and Quality Assurance Standards – Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software
ANSI/ISO/ASQ Q9001:2000	American National Standard Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation and Servicing
ANSI/IPC-A-600	Acceptability of Printed Boards
ASTM E-595	Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment
FAR	Federal Acquisition Regulations
GIDEP S0300-BT-PRO-010	GIDEP Operations Manual
GIDEP S0300-BU-GYD-010	Government-Industry Data Exchange Program Requirements Guide
GMI 1700.2	Goddard Space Flight Center Health, and Safety Program
GPR 1060.2	Management Review and Reporting for Programs and Projects
GPR 8621.1	Reporting of Mishaps, Incidents, Hazards, and Close Calls
GPR 8621.2	Processing Mishap, Incident, Hazard, and Close Call Reports
GPR 8621.3	Mishap, Incident, Hazard, and Close Call Investigation
GPR 8700.4	Technical Review Program
GPR 8700.6	Engineering Peer Reviews
GSFC-STD-7000	General Environmental Verification Standards (GEVS) for Flight Programs and Projects
GSFC S-312-P003	Procurement Specification for Rigid Printed Boards for Space Applications and Other High Reliability Uses

GSFC EEE-INST-002	Instructions for EEE Parts Selection, Screening, and Qualification and Derating
IEEE STD 610.12	IEEE Standard Glossary for Software Engineering Terminology
IEEE STD 730	IEEE Standard for Software Quality Assurance Plans
IEEE STD 982.1	IEEE Standard Dictionary of Measures to Produce Reliable Software
IEEE STD 982.2	IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software
IPC A-600	Acceptability of Printed Boards
IPC-A-610	Acceptability of Electronic Assemblies
IPC/EIA J-STD-001	Requirements for Soldered Electrical and Electronic Assemblies
IPC-2221	Generic Standard on Printed Board Design
IPC-2222	Sectional Design Standard for Rigid Organic Printed Boards
IPC-2223	Sectional Design Standard for Flexible Printed Boards
IPC-6011	Generic Performance Specifications for Printed Boards
IPC-6012	Qualification and Performance Specification for Rigid Printed Boards
IPC-6013	Qualification and Performance Specification for Flexible Printed Boards
IPC-6018	Microwave End Product Board Inspection and Test
ISO 17025	General Requirements for the Competence of Testing and Calibration Laboratories
KHB 1860.1	KSC Ionizing Radiation Protection Program
KHB 1860.2	KSC Non-Ionizing Radiation Protection Program
KNPR 8715.3	KSC Safety Practices Procedural Requirements
MIL-HDBK-217	Reliability Prediction of Electronic Equipment
MIL-HDBK-470	Designing and Developing Maintainable Products and Systems

MIL-HDBK-472	Maintainability Prediction
MIL-PRF-19500	General Specification for Semiconductor Devices
MIL-PRF-38534	General Specification for Hybrid Microcircuits
MIL-PRF-38535	General Specification for Integrated Circuits (Microcircuits) Manufacturing
MIL-PRF-55365/4	General Specification for Established Reliability and Nonestablished Reliability of (Tantalum) Chip Fixed Electrolytic Capacitors
MIL-STD-461	Electromagnetic Emission and Susceptibility Requirement for Control of Electromagnetic Interference
MIL-STD-756	Reliability Modeling and Prediction
MIL-STD-882	System Safety Program Requirements
MIL-STD-883	DoD Test Method Standards for Microcircuits
MIL-STD-981	Design, Manufacturing and Quality Standards for Custom Electromagnetic Devices for Space Applications
MIL-STD-1629	Procedures for Performing a Failure Mode Effects and Criticality Analysis
MSFC 3029	Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments
MSFC CR 5320.9	Payload and Experiment Failure Mode Effects Analysis and Critical Items List Ground Rules
MSFC-HDBK-527	Material Selection List for Space Hardware Systems
NASA RP-1124	Outgassing Data for Selecting Spacecraft Materials
NASA RP-1161	Evaluation of Multi-Layer Printed Wiring Boards by Metallographic Techniques
NFS 1815.201	NASA Federal Acquisition Regulation Supplement Exchanges with Industry before Receipt of Proposals
NFS 1823.7001	NASA Federal Acquisition Regulation Supplement Safety and Health NASA Solicitation Provisions and Contract Clauses

NFS 1815.305	NASA Federal Acquisition Regulation Supplement Source Selection Proposal Evaluation
NFS 1846.401	NASA Federal Acquisition Regulation Supplement Government Contract Quality Assurance General
NHB 1700.1	NASA Safety Policy and Requirements Document
NPD 7120.4	Program and Project Management
NPD 8700.1	NASA Policy for Safety & Mission Success
NPD 8710.2	NASA Safety and Health Program Policy
NPD 8710.3	NASA Policy for Limiting Orbital Debris Generation
NPR 5100.4	NASA FAR Supplement
NPR 7120.5	NASA Program and Project Management Processes and Requirements
NPR 8621.1	NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Record Keeping
NPR 8715.3	NASA Safety Manual
NPR 8000.4	Risk Management Procedural Requirements
NASA-STD 8719.8	Expendable Launch Vehicle Payloads Safety Review Process Standard
NASA-STD 8719.9	NASA Standard for Lifting Devices and Equipment
NASA-STD 8719.13	NASA Software Safety Standard
NASA-STD 8719.14	Guidelines and Assessment Procedures for Limiting Orbital Debris
NASA-STD 8739.1	Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
NASA-STD 8739.2	Workmanship Standard for Surface Mount Technology
NASA-STD 8739.3	Workmanship Standard for Soldered Electrical Connections
NASA-STD 8739.4	Workmanship Standard for Crimping, Interconnecting Cables, Harnesses and Wiring

NASA-STD-8739.5	Workmanship Standard for Fiber Optic Terminations, Cable Assemblies and Installation
NSS 1740.14	Guidelines and Assessment Procedures for Limiting Orbital Debris
S-302-89-01	Procedures for Performing a Failure Mode and Effects Analysis
S-311-M-70	Specification for Destructive Physical Analysis
SAE AS9100	Aerospace Standard, Quality Systems Model for Quality Assurance, Design, Development, Production, Installation and Servicing
SAE JA1002	Software Reliability Program Standard
300-PG-7120.2.1	Mission Assurance Guidelines (MAG) Implementation
302-PG-7120.2.1	Mission Assurance Guidelines Implementation
541-PG-8072.1.2	GSFC Fastener Integrity Requirements
540-PG-8715.1.1	Mechanical Systems Division Safety Manual, Volume I
540-PG-8715.1.2	Mechanical Systems Division Safety Manual, Volume II

18.0 DATA ITEMS DESCRIPTIONS

Table 18-1. DID 1-1: Heritage Hardware Matrix or Report

Title: Heritage Hardware Matrix or Report	**CDRL Number:** 1-1
Reference: Section 1.2	
Use: Documents the use of previously flown spaceflight hardware.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Provide initial matrix or report to GSFC for review and approval 30 days prior to PDR. Updates as developed. Final is due to GSFC for approval 45 days prior to CDR.	
Preparation Information: Prepare a matrix or report detailing what hardware is being considered as heritage for inclusion on this mission. The Matrix or Report shall contain: a. The hardware to be incorporated. b. Introductory pages about the previous flight history including duration, environment, and any flight anomalies. c. Detailed testing history including failures and test anomalies. d. EEE parts selection and testing program used for the hardware. e. FMEA of the hardware. f. As built EEE parts and materials list. g. Comparison of previous environment, radiation requirements, life/duration and testing with the present mission requirements. h. An appendix for supportive data and analyses, if appropriate.	

Table 18-2. DID 2-1: Quality Manual

Title: Quality Manual	**CDRL Number:** 2-1
Reference: Section 2.1	
Use: Documents the developer's QMS.	
Related Documents: ANSI/ISO/ASQC Q9001:1994, ANSI/ISO/ASQC Q9001:2000, SAE AS9100 and ISO 10013.	
Place/Time/Purpose of Delivery: Provide with the proposal for GSFC review. Provide the Quality Manual updates to the GSFC Project Office for review prior to implementation, or Provide with the proposal for information, along with evidence of third party certification/registration of the developer's QMS by an accredited registrar.	
Preparation Information: Prepare a Quality Manual addressing all applicable requirements of relevant quality standard (see above related documents). Refer to ISO 10013 for further guidelines on the preparation of a quality manual. The Quality Manual shall contain: a. The title, approval page, scope and the field of application. b. A table of contents. c. Introductory pages about the organization concerned and the manual itself. d. The quality policy and objectives of the organization. e. The description of the organization, responsibilities and authorities, including the organization responsible for the EEE parts, materials, reliability, safety, and test requirements implementation. f. A description of the elements of the quality system, developer policy regarding each element and developer implementation procedure for each clause or reference(s) to approved quality system procedures. System level procedures shall address the implementation of all requirements cited in this document. g. A definitions section, if appropriate. h. An appendix for supportive data, if appropriate. Quality Manual distribution and changes shall be implemented by a controlled process. The Quality Manual shall be maintained/updated by the developer throughout the life of the contract.	

Table 18-3. DID 2-2: Problem Failure Reports

Title: Problem Failure Reports (PFRs)	**CDRL Number:** 2-2
Reference: Section 2.2.4	
Use: To report failures promptly to the FRB for determination of cause and corrective action.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Provide information to the GSFC Project Office within 24 hours of each occurrence; Provide to GSFC Project Office for approval immediately after developer closure.	
Preparation Information: Reporting of failures shall begin with the first power application at the start of end item acceptance testing of the major component, subsystem, or instrument level (as applicable to the hardware level for which the developer is responsible) or the first operation of a mechanical item. It shall continue through formal acceptance by the GSFC project office and the post-launch operations, commensurate with developer presence and responsibility at GSFC and launch site operations. All failures shall be documented on existing developer PFR form, which shall identify all relevant failure information. PFRs and updated information shall be submitted to GSFC by hard copy or in electronic format. PFRs submitted to the GSFC for closure include a copy of all referenced data and shall have had all corrective actions accomplished and verified.	

Table 18-4. DID 2-3 Subcontractor Verification Matrix

Title: Subcontractor Assurance Verification Matrix	**CDRL Number:** 2-3
Reference: Section 2.2.7	
Use: Summarize subcontracted hardware compliance with the system assurance requirements as defined in the LRO MAR	
Related Documents: 431-RQMT-000174	
Place/Time/Purpose of Delivery: Matrix to be delivered to the project 10 days prior to instrument/SC PSR.	
Preparation Information: Verification Matrix: Document and track adherence to applicable system assurance requirements. Provide supporting documentation showing how each requirement will be verified, and summarize compliance/noncompliance with requirements. It shall show each requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, report reference numbers, etc.	

Table 18-5. DID 3-1: System Safety Program Plan

Title: System Safety Program Plan	**CDRL Number:** 3-1
Reference: Section 3.2.1	

Use:

The approved plan provides a formal basis of understanding between the GSFC Code 302 and the developer on how the System Safety Program will be conducted to meet the applicable launch range safety requirements (ELV launch). The approved plan shall account for all contractually required tasks and responsibilities on an item-by-item basis.

Related Documents:

KNPR 8715.3, "KSC Safety Practices Procedural Requirements"
AFSCM 91-710, "Range Safety User Requirements Manual"

Place/Time/Purpose of Delivery:

The Range User shall submit a draft SSPP to GSFC Code 302 for review and approval at SRR or first program review.

Preparation Information:

The SSPP shall describe in detail tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate and control hazards, or reduce the associated risk to an acceptable level throughout the system life cycle.

Provide a detailed SSPP to describe how the project will implement a safety program in compliance with launch range requirements. Integration of system/facility safety provisions into the SSPP is vital to the early implementation and ultimate success of the safety effort. The SSPP shall:

a. Define the required safety documentation, applicable documents, associated schedules for completion, roles and responsibilities on the project, methodologies for the conduct of any required safety analyses, reviews, and safety package.
b. Provide for the early identification and control of hazards to personnel, facilities, support equipment, and the flight system during all stages of project development including design, fabrication, test, transportation and ground activities.
c. Ensure the program undergoes a safety review process that meets the requirements of NASA-STD-8719.8, "Expendable Launch Vehicle Payloads Safety Review Process Standard." Address compliance with the system safety requirements of range requirements.
d. Address compliance with the baseline industrial safety requirements of the institution, range safety, applicable Industry Standards to the extent practical to meet NASA and OSHA design and operational needs (i.e. NASA STD 8719.9, "Std. for Lifting Devices and Equipment"), and any special contractually imposed mission unique obligations (including applicable safety requirements).
e. Address the software safety effort to identify and mitigate safety-critical software products in compliance with NASA-STD-8719.13 "NASA Software Safety Standard."

Table 18-6. DID 3-2: Safety Requirements Compliance Checklist

Title: Safety Requirements Compliance Checklist	**CDRL Number:** 3-2
Reference: Section 3.2.2	
Use: The checklist shall indicate for each requirement if the proposed design is compliant, non-compliant but meets intent, non-compliant (waiver required) or non-applicable.	
Related Documents: AFSCM 91-710, "Range Safety User Requirements Manual"	
Place/Time/Purpose of Delivery: Provide Safety Requirements Checklist with each submittal of the SAR and/or Safety Data Package/MSPSP.	
Preparation Information: A compliance checklist of all design, test, analysis, and data submittal requirements shall be provided. The following items are included with a compliance checklist. 1. Criteria/requirement. 2. System. 3. Compliance 4. Noncompliance. 5. Not applicable. 6. Resolution. 7. Reference. 8. Copies of all Range Safety approved non-compliances, including waivers and equivalent levels of safety certifications.	

Table 18-7. DID 3-3: Preliminary Hazard Analysis

Title: Preliminary Hazard Analysis	**CDRL Number:** 3-3
Reference: Section 3.2.3.1	

Use:

The developer shall perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to Office of Systems Safety and Mission Assurance (OSSMA) GSFC.

Related Documents:

AFSCM 91-710, "Range Safety User Requirements"
NPR 8715.3, "NASA Safety Manual"
MIL-STD-882, "System Safety Program Requirements" (provides guidance)

Place/Time/Purpose of Delivery:

The developer shall submit the PHA 30 days prior to PDR.

Preparation Information:

Perform and document a PHA, based on the hazard assessment criteria provided in Chapter 3 of NPR 8715.3, to obtain an initial risk assessment of the system. Based on the best available data, including mishap data (if assessable) from similar systems and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable level shall be included. The PHA shall consider the following for identification and evaluation of hazards at a minimum:

a. Hazardous components.
b. Environmental constraints including the operating environments.
c. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures.
d. Facilities, real property installed equipment, support equipment.
e. Safety related equipment, safeguards, and possible alternate approaches.
f. Safety related interface considerations among various elements of the system. This shall include consideration of the potential contribution by software to subsystem/system mishaps. Safety design criteria to control safety-critical software commands and responses shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.
g. Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.

Additionally, the PHA shall include a system description and a description of the methodology used to develop the analysis.

Table 18-8. DID 3-4 Operations Hazard Analysis

Title: Operations Hazard Analysis	**CDRL Number:** 3-4
Reference: Section 3.2.3.4	

Use:

The operations hazard analysis (OHA) shall consider safety requirements for personnel, procedures, and equipment used during testing, transportation, storage, and integration operations in the 7/10/15/29 complex at GSFC. An engineering design analysis shall be accomplished for review and for developing recommendations concerning system integration and test operations.

Related Documents:

540-PG-8715.1.1, "Mechanical Systems Division Safety Manual – Volume I"
540-PG-8715.1.2, "Mechanical Systems Division Safety Manual – Volume II"

Place/Time/Purpose of Delivery:

The customer shall provide a preliminary OHA 45 days prior to shipping to GSFC. A final version must be submitted 15 days prior to shipping and must be approved by Code 302 prior to initiating any I&T activities. During I&T activities, a Hazard Tracking Log (HTL) shall be used to track and close all remaining items.

Note: Closure methodology for the HTL is the same as for the VTL in DID 3-7.

Preparation Information:

The OHA shall include the following information:

1.0 Introduction
- a. Provide an abstract summarizing the major findings of the analysis and the proposed corrective or follow-up actions.
- b. Define any special terms, acronyms, and/or abbreviations used.

2.0 System Description
- a. Provide a description of the system hardware and configuration. List components of subsystems.
- b. The most recent schedules for integration and testing of the instrument/SC.
- c. Photographs, diagrams, and sketches should be included to support the test.

3.0 Analysis of System Hazards
- a. The analysis shall identify all real or potential hazards presented to personnel, equipment, and property during I&T processing.
- b. A listing of all identified hazards shall be provided in a tabulated format. Each hazard shall be numbered and shall include the following information:
  - (1) System Component/Phase. The particular phase/component that the analysis is concerned with. This could be a system, subsystem, component, operating/maintenance procedure or environmental condition.
  - (2) System Description and Hazard Identification, Indication.
    - (a) A description of what is normally expected to occur as the result of operating the component/subsystem or performing the operating/maintenance action.
    - (b) A complete description of the actual or potential hazard resulting from normal actions or equipment failures. Indicate whether hazard will cause personnel injury and/or equipment damage.
    - (c) A description of crew indications which include all means of identifying the hazard to operating or maintenance personnel.
    - (d) A complete description of the safety hazards of software controlling hardware systems where the hardware effects are safety critical.
  - (3) Effect on System. The detrimental results an uncontrolled hazard could inflict on the whole system.
  - (4) Risk Assessment. A risk assessment for each hazard as defined in paragraph shall be provided.
  - (5) Caution and Warning Notes. A complete list of specific warnings, cautions, procedures required in operating and maintenance manuals, training courses, and test plans.

(6) Status/Remarks.
(a) The status of actions to implement the recommended, or other, hazard controls.
(b) Any information relating to the hazard, not covered in the other blocks, for example, applicable documents, previous failure data in similar systems, or administrative directions.

4.0 References. List all pertinent references such as test reports, preliminary operating and maintenance manuals, and other hazard analysis.

5.0 Appendices. The appendix will contain charts, graphs, or data which are too cumbersome for inclusion in the previous sections, or are applicable to more than one section. It may also contain detailed formulation or analysis which is more conveniently placed in an appendix.

Table 18-9. DID 3-5 Safety Assessment Report

Title: Safety Assessment Report	**CDRL Number:** 3-5
Reference: Section 3.3	

Use:

The Safety Assessment Report (SAR) is used to document a comprehensive evaluation of the mishap risk being assumed prior to the testing or operation of an instrument or subsystem not being developed by the SC contractor. The SAR will be provided to the SC contractor as an input to their preparation of the MSPSP, which is one of the media through which missile system prelaunch safety is obtained.

Related Documents:

AFSCM 91-710, "Range Safety User Requirements Manual"

Place/Time/Purpose of Delivery:

SAR delivery shall support the SC contractor's MSPSP submittal schedule. The preliminary MSPSP is due at PDR, with update at CDR, and final 60 days prior to PSR. The adequate support MSPSP development, the preliminary SAR shall be delivered 30 days after instrument/subsystem PDR, shall be updated 30 days prior to instrument/subsystem CDR, and the final SAR shall be delivered 30 days prior to instrument/subsystem delivery.

Preparation Information:

The SAR will identify all safety features of the hardware, software, and system design as well as procedural, hardware, and software related hazards that may be present in the system being acquired. This includes specific procedural controls and precautions that shall be followed. The safety assessment will summarize the following information:

1. The safety criteria and methodology used to classify and rank hazards and any assumptions upon which they were based or derived, including the definition of acceptable risk (as specified by Range Safety).
2. The results of those analyses and tests performed to identify hazards inherent in the system, including:
   a. Those hazards that still have a residual risk and the actions taken to reduce the associated risk to a level contractually specified as acceptable
   b. Results of tests conducted to validate safety criteria, requirements, and analyses
3. Hazard reports documenting the results of the safety program efforts, including a list of all significant hazards, including specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment. NOTE: List categorization shall denote whether the risks may be expected under normal or abnormal operating conditions.
4. Any hazardous materials generated by or used in the system.
5. The conclusion, with signed statement, that all identified hazards have been eliminated or their associated risk has been controlled to acceptable levels, and the system is ready to test, operate, or proceed to the next phase.
6. In order to aid the SC developer/observatory integrator in completing an orbital debris assessment, it is necessary to identify any stored energy sources (e.g., pressure vessels, batteries, etc.) that can be passivated at end of life.
7. Recommendations applicable to hazards at the interface of Range User systems with other systems.

Table 18-10. DID 3-6 Missile System Pre-Launch Safety Package

Title: Missile System Pre-Launch Safety Package	**CDRL Number:** 3-6

Reference: Section 3.4

Use:

Provide a detailed description of the payload design, sufficient to support hazard analysis results, hazard analysis method, and other applicable safety related information. The developer shall include analyses identifying the ground operations hazards associated with the flight system, GSE, and their interfaces. The developer shall take measures to control and/or minimize each identified significant hazard.

Related Documents:

AFSCM 91-710, "Range Safety User Requirements Manual"

Note: Other launch vehicle and/or contractor or commercial facility requirements may apply.

Place/Time/Purpose of Delivery:

Provide preliminary MSPSP 30 days after PDR package, an updated MSPSP 30 days prior to CDR, and final 60 days prior to PSR. (See applicable launch range and launch vehicle requirements for details.)

Preparation Information:

MSPSP shall follow the guidance in AFSCM 91-710, and include the following information:

1. Introduction. State, in narrative form, the purpose of the MSPSP.
2. System Description. This section may be developed by referencing other program documentation such as technical manuals, System Program Plan, System Specifications, etc.
3. System Operations. A description of:
   a. Or reference to the procedures for operating, testing, and maintaining the system. Discuss the safety design features and controls incorporated into the system as they relate to the operating procedures.
   b. Any special safety procedures needed to assure safe operations, test, and maintenance, including emergency procedures.
   c. Anticipated operating environments and any specific skills required for safe operation, test, maintenance, transportation, or disposal.
   d. Any special facility requirements or personal equipment to support the system.
4. Systems Safety Engineering Assessment. This section shall include:
   a. A summary or reference of the safety criteria and methodology used to classify and rank hazardous conditions.
   b. A description of, or reference to, the analyses and tests performed to identify hazardous conditions inherent in the system.
   c. A list of all hazards by subsystem or major component level that have been identified and considered from program inception.
   d. A discussion of the hazards and the actions taken to eliminate or control these items.
   e. A discussion of the effects of these controls on the probability of occurrence and severity level of the potential mishaps.
   f. A discussion of the residual risks that remain after the controls are applied or for which no controls could be applied.
   g. A discussion of, or reference to, the results of tests conducted to validate safety criteria requirements and analyses. These items shall be tracked and closed-out via a VTL.
5. Conclusions and Recommendations. This section shall include:
   a. A short assessment of the results of the safety program efforts. A list of all significant hazards, including specific safety recommendations or precautions required to ensure the safety of personnel and property.
   b. For all hazardous materials generated by or used in the system, the following information shall be included.
      (1) Material identification as to type, quantity, and potential hazards.

(2) Safety precautions and procedures necessary during use, storage, transportation, and disposal.
(3) A copy of the Material Safety Data Sheet (OSHA Form 20 or DD Form 1813) as required.

c. Reference material, to include a list of all pertinent references, such as test reports, preliminary operating manuals, and maintenance manuals.
d. A statement signed by the Contractor System Safety Manager and the Program Manager, certifying that all identified hazards have been eliminated or controlled, and that the system is ready to test, operate, or proceed to the next acquisition phase. In addition, include recommendations applicable to the safe interface of this system with other systems.

Table 18-11. DID 3-7: Verification Tracking Log

Title: Verification Tracking Log	**CDRL Number:** 3-7
Reference: Section 3.5	
Use: To provide a Hazard Control and Verification Tracking process, or "closed-loop system," to assure safety compliance has been satisfied in accordance to applicable launch range safety requirements.	
Related Documents: AFSCM 91-710, "Range Safety User Requirements Manual"	
Place/Time/Purpose of Delivery: Provide hazard control verification and tracking system in accordance with AFSCM 91-710 and applicable launch site range safety requirements. Documented methods of hazard controls shall be submitted with the preliminary MSPSP and updated with each consecutive submittal. All open hazard control verification items must be closed in accordance with applicable launch site range safety requirements before launch, and individual items shall be closed with appropriate documentation verifying that the stated hazard control has been implemented, and shall be completed prior to first operational use.	
Preparation Information: Provide documentation that demonstrates the process of verifying the control of all hazards by test, analysis, inspection, similarity to previously qualified hardware, or any combination thereof. All verifications listed on the hazard reports shall reference the tests/analyses/inspections. Results of these tests/analyses/inspections shall be available for review and submitted in accordance with the contract schedule and applicable launch site range safety requirements. The VTL shall contain the following information in tabular format: a. Log b. Hazard report number c. Safety verification number d. Description (Identify procedures/analyses by number and title) e. Constraints on Launch Site Operations f. Independent Verification Required (i.e., mandatory inspection points)? Yes/No g. Scheduled completion date h. Completion date i. Method of Closure	

Table 18-12. DID 3-8: Ground Operations Procedures

Title: Ground Operations Procedures	**CDRL Number:** 3-8
Reference: Section 3.6	
Use: All ground operations procedures to be used at GSFC facilities, other integration facilities, or the launch site shall be submitted to the GSFC Project Safety Manager for review and concurrence.	
Related Documents: AFSCM 91-710, "Range Safety User Requirements Manual" KNPR 8715.3, "KSC Safety Practices Procedural Requirements" Note: Other launch vehicle and/or contractor or commercial facility requirements may apply.	
Place/Time/Purpose of Delivery: Launch Range Procedures: Provide 60 days prior to PDR, final 60 days before PSR, and submit to Range Safety 45 days prior to use. GSFC Facility Procedures: Provide all GSFC In-House procedures to GSFC Code 302 for review 7 days prior to first operational use. GSFC Code 302 will approve all hazardous operational procedures.	
Preparation Information: All hazardous operations, as well as the procedures to control them, shall be identified and highlighted. All launch site procedures shall comply with the applicable launch site safety regulations.	

Table 18-13. DID 3-9 Safety Variances

Title: Safety Variances	**CDRL Number:** 3-9
Reference: Section 3.7	
Use: The hardware developer shall submit to GSFC Code 302 an associated safety noncompliance request that identifies the hazard and shows the rationale for approval of noncompliance when a specific safety requirement cannot be met, as defined in the applicable launch site safety regulation. Range Safety concurrence may be required for the noncompliance request to be approved.	
Related Documents: AFSCM 91-710, "Range Safety User Requirements Manual" KNPR 8715.3, "KSC Safety Practices Procedural Requirements" NASA Problem Reporting/Problem Failure Reporting Module Web-based Online System	
Place/Time/Purpose of Delivery: As identified to the GSFC Project Safety Manager.	
Preparation Information: The noncompliance request shall include the following information resulting from a review of each waiver or deviation request. a. A statement of the specific safety requirement and its associated source document name and paragraph number, as applicable, for which a waiver or deviation is being requested. b. A detailed technical justification for the exception. c. Analyses to show the mishap potential of the proposed alternate requirement, method, or process, as compared to the specified requirement. d. A narrative assessment of the risk involved in accepting the waiver or deviation. When it is determined that there are no hazards, the basis for such determination shall be provided. e. A narrative on possible ways of reducing hazard severity and provability, and existing compliance activities (if any). f. Starting and expiration date for waiver/deviation.	

Table 18-14. DID 3-10: Orbital Debris Assessment

Title: Orbital Debris Assessment	**CDRL Number:** 3-10
Reference: Section 3.9	
Use: Ensure NASA requirements for post mission orbital debris control are met.	
Related Documents: NPD 8710.3, "NASA Policy for Limiting Orbital Debris Generation" NSS 1740.14, "Guidelines and Assessment Procedures for Limiting Orbital Debris"	
Place/Time/Purpose of Delivery: Provide preliminary assessment prior to PDR, and final 45 days prior to CDR. Deliveries should be made jointly to GSFC Code 302, NASA HQ OSSMA, NASA HQ Enterprise Associate Administrator, and the Johnson Space Center (JSC) Orbital Debris Office. Additional info may be required after review of the report, and should be provided as soon as possible to complete the assessment.	
Preparation Information: The assessment shall be done in accordance with NSS 1740.14. The preliminary debris assessment shall be conducted to identify areas where the program or project might contribute debris, and to assess this contribution relative to the guidelines in so far as feasible. Prior to CDR another debris assessment shall be completed. This report shall comment on changes made since the preliminary report. The level of detail shall be consistent with available information of design and operations. When design changes are made after CDR that impact the potential for orbital debris generation, the updated of the debris assessment report shall be prepared, approved, and coordinated with the Office of System Safety and Mission Assurance. Orbital Debris Assessment Software is available for download from JSC at: http://sn-callisto.jsc.nasa.gov/mitigate/das/das.html	

Table 18-15. DID 4-1: Reliability Program Plan

Title: Reliability Program Plan	**CDRL Number:** 4-1
Reference: Section 4.2	
Use: To provide planning and control for the reliability program.	
Related Documents: NPD 8720.1, "NASA Reliability and Maintainability (R&M) Program Policy" NASA-STD-8729.1, "Planning, Developing and Managing an Effective Reliability and Maintainability Program"	
Place/Time/Purpose of Delivery: Preliminary to be included with proposal for GSFC review and evaluation. Draft 30 days after contract award for GSFC review. Final 30 days before developer PDR for GSFC review and approval. Updates as required, including changes for GSFC review and approval.	
Preparation Information: The RPP shall describe how reliability program requirements shall be complied with, and shall include the following: a. Charts and statements describing the organizational responsibilities and functions associated with conduct of the reliability program and each of the tasks to be performed as part of the reliability program. A summary (matrix or other brief form) shall be included which indicates for each reliability program requirement, the principal organization responsible for implementation and the specific organization responsible for generating the necessary documentation. The summary shall identify each organization that has approval, oversight, or review authority relative to documents generated. The narrative shall include the following for each task: 1. Duties of each organizational element relative to each task and its accomplishment 2. Delineation of interfaces in responsibilities and functions where more than one organizational element is involved 3. Relationship of the reliability organization to each of the other organizational elements performing reliability tasks with the lines of authority and oversight clearly identified b. Narrative descriptions, time or milestone schedules, and supporting documents, which describe in detail the plan for execution and management of each task in the reliability, program. Directives, methods and procedures relative to each task shall be documented in the plan.	

Table 18-16. DID 4-2: Probabilistic Risk Assessment

Title: Probabilistic Risk Assessment	**CDRL Number:** 4-2
Reference: Sections 4.3	

Use:

Probabilistic Risk Assessments (PRAs) provide a structured, disciplined approach to analyzing system risk to enable management decisions that ensure mission success, improve safety in design, operation maintenance and upgrade, improve performance, and reduce design, operation, and maintenance costs.

Related Documents:

NPR 8705.4, "Risk Classification for NASA Payloads"
NPR 8705.5, "Probabilistic Risk Assessment Procedures for NASA Programs and Projects"

Place/Time/Purpose of Delivery:

PRA Planning Document due 6 months before PDR for review and approval.
Preliminary PRA due 30 days before PDR for review.
Final PRA due 30 days after CDR for approval.
Updates due as changes are made and between CDR and delivery, for approval.

Preparation Information:

The PRA prepared shall identify what types of analyses are to be performed for each scenario and what modeling tools and techniques are to be used (e.g., Master Logic Diagrams [MLD], FMEAs, FTAs, Event Tree Analyses [ETA], and Event Sequence Diagrams).

The PRA shall include:

a. A definition of the objective and scope of the PRA, and development of end-states-of-interest to the decision maker.
b. Definition of the mission phases and success criteria.
c. Initiating event categories.
d. Top level scenarios.
e. Initiating and pivotal event models (e.g., fault trees and phenomenological event models).
f. Data development for probability calculations.
g. An integrated model and quantification to obtain risk estimates.
h. An assessment of uncertainties.
i. A summary of results and conclusions, including a ranking of the lead contributors to risk.

Table 18-17. DID 4-3: Failure Mode and Effects Analysis and Critical Items

Title: Failure Mode and Effects Analysis and Critical Items List	**CDRL Number:** 4-3
Reference: Sections 4.4.1	
Use: The Failure Mode and Effects Analysis (FMEA) is a reliability analysis to evaluate design relative to requirements, to identify single point failures, and to identify hazards to guide preventative design actions. The Critical Items List (CIL) provides a list of critical items, which require the highest level of attention in design, fabrication, verification, and problem correction during the development, handling, and mission use of the system.	
Related Documents: FAP P-302-720, "Performing a Failure Mode and Effects Analysis" CR 5320.9, "Payload and Experiment Failure Mode Effects Analysis and Critical Items List Ground Rules" MIL-STD-1629, "Procedures for Performing an FMECA"	
Place/Time/Purpose of Delivery: Preliminary 30 days before PDR for GSFC review. Final 30 days before CDR for GSFC review. Updates as required, including changes, for GSFC review.	
Preparation Information: The FMEA report shall document the reliability analysis including approach, methodologies, results, conclusions, and recommendations. The report shall include objectives, level of the analysis, ground rules, functional description, functional block diagrams, reliability block diagrams, bounds of equipment analyzed, reference to data sources used, identification of problem areas, single-point failures, recommended corrective action, and work sheets as appropriate for the specific analysis being performed. The CIL shall include item identification, cross-reference to FMEA line items, and retention rationale. Appropriate retention rationale may include design features, historical performance, acceptance testing, manufacturing product assurance, elimination of undesirable failure modes, and failure detection methods.	

Table 18-18. DID 4-4: Fault Tree Analysis

Title: Fault Tree Analysis	**CDRL Number:** 4-4
Reference: Sections 4.4.2	
Use: A fault tree is an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in context of its environment and operation to find all credible ways in which the undesired event can occur. The analysis provides a methodical approach to understanding they system, its operation, and the environment it will operate in. Through this understanding, informed decisions regarding system design and operation can be made.	
Related Documents: NUREG-0492, "Fault Tree Handbook"	
Place/Time/Purpose of Delivery: Preliminary 30 days before PDR for GSFC review. Final 30 days before CDR for GSFC review. Updates as required, including changes, for GSFC review.	
Preparation Information: The Fault Tree Analysis (FTA) Report shall contain: a. Ground rules for the analysis, including definitions of the undesirable end states analyzed. b. References to documents and data used. c. The fault tree diagrams. d. Statement of the results and conclusions.	

Table 18-19. DID 4-5: Parts Stress Analysis

Title: Parts Stress Analysis	**CDRL Number:** 4-5
Reference: Section 4.4.3	
Use: Provides EEE parts stress analyses for evaluating circuit design and conformance with derating guidelines. Demonstrates that environmental operational stresses on parts comply with project derating requirements.	
Related Documents: NASA Parts Selection List	
Place/Time/Purpose of Delivery: Final 45 days before GSFC CDR for GSFC review. Updates to include changes as required for GSFC review.	
Preparation Information: The stress analysis report shall contain: a. Ground rules for the analysis. b. References to documents and data used. c. Statement of the results and conclusions. d. Analysis worksheets, which shall include (at a minimum): • Part identification (traceable to circuit diagrams) • Environmental conditions assumed (consider all expected environments) • Rated stress • Applied stress (consider all significant operating parameter stresses at the extremes of anticipated environments) • Ratio of applied-to-rated stress	

Table 18-20. DID 4-6: Worst Case Analysis

Title: Worst Case Analysis	**CDRL Number:** 4-6
Reference: Section 4.4.4	
Use: To demonstrate the adequacy of margin in the design of electronic and electrical circuits, optics, and electromechanical and mechanical items.	
Related Documents: NPD 8720.1, "NASA Reliability and Maintainability (R&M) Program Policy" NASA-STD-8729.1, "Planning, Developing and Managing an Effective R&M Program"	
Place/Time/Purpose of Delivery: Available 30 days prior to component CDR. Updates with design changes.	
Preparation Information: These analyses shall address the worst case conditions for the analysis performed on each component. Each analysis shall cover the mission life and consider the critical parameters set at maximum and minimum limits, including the effect of environmental stresses on the operational parameters being evaluated.	

Table 18-21. DID 4-7: Reliability Assessments and Predictions

Title: Reliability Assessments and Predictions	**CDRL Number:** 4-7
Reference: Section 4.4.5	
Use: Reliability analysis to assist in evaluating alternative designs and to identify potential mission limiting elements that may require special attention.	
Related Documents: MIL-STD-756, "Reliability Modeling and Prediction" MIL-HDBK-217, "Reliability Prediction of Electronic Equipment" RADC-TR-85-229, "Reliability Prediction for Spacecraft"	
Place/Time/Purpose of Delivery: Preliminary 30 days before PDR for GSFC review. Final 30 days before CDR for GSFC review. Updates as required, including changes, for GSFC review.	
Preparation Information: The assessment report shall document the methodology and results of comparative reliability assessments including mathematical models, reliability block diagrams, failure rates and definitions, degraded operating modes, trade-offs, assumptions, and any other pertinent information used in the assessment process. Format of the report is not critical, but should incorporate good engineering practices and clearly show how reliability was considered as a discriminator in the design process.	

Table 18-22. DID 4-8: Trend Analysis

Title: Trend Analysis	**CDRL Number:** 4-8
Reference: Section 4.5.1	
Use: To monitor parameters on components and subsystems that relate to performance stability (any deviations from nominal that could indicate trends) throughout the normal test program. Operational personnel continue to monitor trends through mission duration.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: List of parameters to be monitored at time of CDR for information. Trend Analysis Reports at time of PER and FRR for information.	
Preparation Information: The system for selecting parameters related to performance stability, recording any changes from the nominal, analyzing trends, and coordinating results with design and operational personnel shall be documented. The list of parameters to be monitored, updates to the list, and trend reports shall be prepared. In addition, a log shall be kept for each black box or unit (e.g. tape recorder) of the accumulated operating time. The log shall contain the following minimum information: identification, serial number, total operating time since assembly of unit, total operating time at each parameter observation, and total additional operating time for the unit prior to launch.	

Table 18-23. DID 4-9: Limited-Life Items List

Title: Limited Life Items List	**CDRL Number:** 4-9
Reference: Sections 4.6, 11.5	
Use: Defines and tracks the selection, use and wear of limited-life items, and the impact on mission operations.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Preliminary 30 days before PDR for LRO review. Final 30 days before CDR for approval. Updates as changes are made, and between CDR and Delivery, for approval.	
Preparation Information: List limited-life items and their impact on mission parameters. Define expected life, required life, duty cycles, and basis for selecting and using the items. Include selected structures, thermal control surfaces, solar arrays, and electromechanical devices. Atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue are used to identify limited-life control surfaces and structural items. When aging, wear, fatigue, and lubricant degradation limit their life, include batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, hinge assemblies, drive assemblies, gyros, actuators, and scan devices.	

Table 18-24. DID 5-1: Software Assurance Plan

Title: Software Assurance Plan	**CDRL Number:** 5-1
Reference: Sections 5.2, 5.8	
Use: The Software Assurance Plan (SAP) documents the Software Assurance roles and responsibilities, surveillance activities, supplier controls, records collection, maintenance and retention, training, and risk management.	
Related Documents: IEEE Standard 730-2002, "Software Quality Assurance Plans"	
Place/Time/Purpose of Delivery: Draft due no later than 60 days prior to SRR. Baseline due two weeks prior to SRR. Updated periodically through the life cycle, if necessary.	
Preparation Information: The SAP shall follow the format as specified in IEEE Standard 730-2002, it shall include: a. Purpose b. Reference documents and definitions c. Management d. Documentation e. Standards, practices, conventions, and metrics f. Software reviews g. Test h. Problem reporting and corrective action i. Tools, techniques, and methodologies j. Media control k. Supplier control l. Records collection, maintenance, and retention m. Training n. Risk management o. SAP change procedure and history	

Table 18-25. DID 5-2: Software Management Plan

Title: Software Management Plan	**CDRL Number:** 5-2
Reference: Sections 5.2, 5.2.2, 5.4, 5.8	
Use: This data item provides an outline for the Software Management Plan. The plan documents the software development processes and procedures, software tools, resources, and deliverables throughout the development life cycle.	
Related Documents: IEEE Standard 1058-1998	
Place/Time/Purpose of Delivery: Draft due no later than 60 days prior to SRR. Baseline due two weeks prior to SRR. Updated periodically through the life cycle, if necessary.	
Preparation Information: The Software Management Plan shall include/address: a. Introduction – Purpose, scope, definitions and references b. Project Organization and Responsibilities – Resources and schedules c. Software development overview d. Software development activities by life cycle – 1) development and test environment, 2) Tools, techniques and methodologies, 3) Software standards and development processes e. Software Configuration Management f. Software assurance g. Software Testing h. Software Reviews i. Risk Management j. Software Metrics k. Delivery and Operational Transition l. Software Maintenance m. Software Deliverables n. Training	

Table 18-26. DID 5-3: Software Configuration Management Plan

Title: Software Configuration Management Plan	**CDRL Number:** 5-3
Reference: Section 5.4	
Use: The Software Configuration Management (SCM) Plan defines the SCM system, roles and responsibilities, activities, schedules, resources, and maintenance of the plan.	
Related Documents: ANSI-IEEE Standard 828-1998, "IEEE Standard for Software Configuration Management Plans" ANSI-IEEE Standard 1042-1987, "Guide to Software Configuration Management"	
Place/Time/Purpose of Delivery: Draft due no later than 60 days prior to SRR. Baseline due two weeks prior to SRR. Updated periodically through the life cycle, if necessary.	
Preparation Information: The SCM Plan may be contained within the CM plan, but must contain the following information. The SCM Plan shall follow the below format: a. Introduction (purpose, scope, definitions, and references) b. SCM Management Overview (organization, responsibilities, and interfaces and relationships to the software life cycle) c. Software Configuration Management activities (Configuration identification, configuration control, configuration status accounting, configuration audits, interface control, and subcontractor control in that order) d. Software Configuration Management Schedules e. Software Configuration management Resources (tools, techniques, equipment, personnel, and training) f. Software Configuration Management Plan Maintenance	

Table 18-27. DID 5-4: Software Reliability Plan

Title: Software Reliability Plan	**CDRL Number:** 5-4
Reference: Section 5.2.3	
Use: The Software Reliability Plan documents the activities to be undertaken to achieve the software reliability requirements, and describes the activities required to demonstrate that the software reliability requirements have been verified.	
Related Documents: SAE JA 1002, "Software Reliability Program Standard" IEEE Standard 982.1 IEEE Standard 982.2	
Place/Time/Purpose of Delivery: Draft due no later than 60 days prior to SRR. Baseline due two weeks prior to SRR. Updated periodically through the life cycle, if necessary.	
Preparation Information: The Software Reliability Plan shall include/address: a. Allocating reliability requirements to software. b. The strategy for software reliability achievement. c. The techniques, methods and tools (including measurements to be used for the evaluation of software reliability at each life cycle phase). d. Risk analysis for the software reliability objectives. e. Identification of database tools that support data collection, analysis, and storage. f. The identification, selection, and integration of COTS software. g. The means by which staff, including subcontractors, are informed of their specific responsibilities in meeting software reliability requirements. h. Specific training activities related to reliability models, methods and techniques. i. The procedures for software reliability progress reporting. j. The distribution of resources employed to address software reliability issues, including the involvement of the customer and any third party. k. The timing of the elements of the Software Reliability Plan relative to the System Reliability Plan.	

Table 18-28. DID 5-5: Software Requirements Specification

Title: Software Requirements Specification	**CDRL Number:** 5-5
Reference: Section 5.2	
Use: The Software Requirements Specification documents all software requirements (e.g. functional, performance, software safety, and security), assumptions and dependencies, design and implementation constraints, delivery and installation requirements, and complete requirements traceability to parent requirements or system requirements.	
Related Documents: IEEE/EIA 12207.1-1997	
Place/Time/Purpose of Delivery: Draft due no later than 60 days prior to SRR. Baseline due two weeks prior to SRR. Updated periodically throughout the life cycle, as needed by requirement changes.	
Preparation Information: When developing requirements, requirement characteristics include correct, unambiguous, complete, consistent, verifiable, modifiable, and traceable (per IEEE STD 830-1998, Recommended Practice for Software Requirements Specifications). The Software Requirements Specification shall meet the intent of IEEE/EIA 12207.1-1997: a. Introduction, Scope, and Applicable Documents b. Software Functional Overview and flow c. Functional Requirements d. External and Internal Requirements e. Performance Requirements f. Software Safety Requirements g. Security and Privacy Requirements h. Quality Requirements i. Delivery, Installation, and Environmental Requirements j. Computer Hardware and Software Resources and Requirements k. Assumptions and Dependencies l. Design and Implementation Constraints m. Qualification Methods and Acceptance Criteria (may be referenced) n. Requirements Traceability	

Table 18-29. DID 7-1: Risk Management Plan

Title: Risk Management Plan	**CDRL Number:** 7-1
Reference: Section 7.3	
Use: The Risk Management Plan (RMP) defines the CRM process by which the developer identifies, evaluates, and minimizes the risks associated with program, project, and/or mission goals.	
Related Documents: GPG 7120.4, "Risk Management" NPR 8000.4, "Risk Management Procedural Requirements"	
Place/Time/Purpose of Delivery: Preliminary 30 days before PDR for GSFC review. Final 30 days before CDR for GSFC review. Updates as required, including changes, for GSFC review.	
Preparation Information: The RMP shall be a configuration controlled document. The RMP shall include: a. Introduction. Specify the project risk objectives and policy toward risk. Explain the purpose, scope, assumptions, constraints, key ground rules, and policy pertaining to the CRM process. b. Overview of Process. Provide an overview of the CRM process and information flow, describe how the CRM process integrates and relates to other project management and system engineering activities. Include general risk mitigation strategies to be used throughout the project life cycle. c. Organization. Show the organization, roles, and responsibilities of program, project, customer, and supplier key personnel with regard to CRM. Document how team members will be trained in the application of CRM methodology. d. Process Details. Provide the CRM process details and related procedures, methods, tools, and metrics. Include the specific methodologies to be used for activities of CRM (identify, analyze, plan, track, control, communicate and document) either here, or in an appendix. Include the process to be used for continual assessment of the Risk Profile. Describe how risk information will be communicated both internally to the project staff and throughout the NASA management chain. e. Documentation of Risks. Specify the format and data elements that will comprise the project Risk List (and/or Risk Database), how configuration control will be applied, and how the list will be used and updated. State how team members will be able to access the current list at any time. Include in the RMP the initial set of identified risks and the action plan (for research acceptance, tracking, or mitigation) for each risk. f. Appendix. Material that is too detailed or sensitive to be placed in the main body of the text may be place in an appendix or included as a reference. Include the appropriate reference in the main body of the text. Appendices may be bound separately, but are considered to be part of the document and shall be place under CM control as such. Include an alphabetized list of the definitions for abbreviations and acronyms used in this document. Include an alphabetized list of definitions for special terms used in the document (i.e., terms used in a sense that differs from, or is more specific than, the common usage for such terms).	

Table 18-30. DID 9-1: System Performance Verification Plan

Title: System Performance Verification Plan	**CDRL Number:** 9-1
Reference: Section 9.2.1	
Use: Provides the overall approach for achieving the verification program. Defines the specific tests, analyses, calibrations, alignments, etc. that will demonstrate the hardware complies with mission requirements.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Preliminary with proposal for GSFC review. Final at CDR for GSFC approval. Updates as required.	
Preparation Information: Describes the approach (test, analysis, etc.) that will be used to verify that the hardware/software complies with mission requirements. If verification relies on tests or analyses at other assembly levels, describe the relationships. A section of the plan shall be a "System Performance Verification Matrix" summarizing the flow-down of system specification requirements that stipulates how each requirement will be verified and the compliance/noncompliance with requirements. It shall show each specification requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, report reference numbers, etc. The System Performance Verification Matrix may be a separate document. The System Performance Verification Plan shall include a section describing the environmental verification program. This shall include level of assembly, item configuration, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, appropriate functional operations, personnel responsibilities, and requirements for procedures and reports. For each analysis activity, include objectives, a description of the mathematical model, assumptions on which the model will be based, required output, criteria for assessing the acceptability of results, interaction with related test activity, and requirements for reports. Provide an operational methodology for controlling, documenting, and approving activities not part of an approved procedure. Plan shall establish controls to prevent accidents that could damage or contaminate hardware or facilities or cause personal injury. The controls shall include real-time decision-making mechanisms for continuation or suspension of testing after malfunction, and a method for determining retest requirements, including an assessment of the validity of previous tests. Include a test matrix that summarizes all tests to be performed on each component, each subsystem, and the payload. Include tests on engineering models performed to satisfy qualification requirements. Define pass/fail criteria. The Environmental Test Plan section shall include an Environmental Test Matrix that summarizes all environmental tests that will be performed showing the test and the level of assembly. Tests on development/engineering models performed to satisfy qualification requirements shall be included in this matrix. The Environmental Verification Plan may be a separate document (instead of a section of the System Performance Verification Plan). As an adjunct to the environmental verification program, an Environmental Test Matrix summarizing all tests performed and, showing the test and the level of assembly will be maintained. The System Performance Verification Plan shall include an Environmental Verification Specification section that stipulates the specific environmental parameters used in each test or analysis required by the Verification Plan. Contains the specific test and analytical parameters associated with each of the tests and analyses required by the Verification Plan. Payload oddities and interactions with the launch vehicle shall be considered when defining quantitative environmental parameters under which the hardware elements must meet their performance requirements.	

Table 18-31. DID 9-2: Performance Verification Procedure

Title: Performance Verification Procedure	**CDRL Number:** 9-2
Reference: Section 9.2.6	
Use: Describes how each test activity defined in the Verification Plan will be implemented.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: 30 days prior to test for GSFC approval.	
Preparation Information: Describe the configuration of the tested item and the step-by-step functional and environmental test activity conducted at the unit/component, subsystem/instrument, and payload levels. Give details such as instrumentation monitoring, facility control sequences, test article functions, test parameters, quality control checkpoints, pass/fail criteria, data collection, and reporting requirements. Address safety and contamination control provisions. A methodology shall be provided for controlling, documenting, and approving all activities not part of an approved procedure, and shall establish controls for preventing accidents that could cause personal injury or damage to hardware and facilities.	

Table 18-32. DID 9-3: Verification Reports

Title: Verification Reports	**CDRL Number:** 9-3
Reference: Sections 9.2.7, 9.2.8	
Use: Summarizes compliance with system specification requirements and/or provides a summary of testing and analysis results (including conformance, nonconformance, and trend data).	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Verification Reports: Preliminary report 72 hours after test, for GSFC information. Final report 30 days after verification activity, for GSFC information. System Performance Verification Report: Preliminary at CDR. Final report 30 days following on-orbit check-out.	
Preparation Information: Verification Report: Provide after each unit/component, subsystem/instrument, and payload verification activity. For each analysis activity, the report shall describe the degree to which the objectives were accomplished, how well the mathematical model was confirmed by the test data, and other key results.	

Table 18-33. DID 10-1: Printed Wiring Board Test Coupons

Title: Printed Wiring Board Test Coupons	**CDRL Number:** 10-1
Reference: Section 10.4.2.1	
Use: Validates printed wiring boards (PWBs) procured for space flight and mission critical ground use are fabricated in accordance with applicable workmanship standards.	
Related Documents: IPC-6011, "Generic Performance Specifications for Printed Boards" IPC-6012B, "Qualification and Performance Specification for Rigid Printed Boards" product to meet requirements of the Performance Specification Sheet for Space and Military Avionics IPC-6013, "Qualification and Performance Specification for Flexible Printed Boards" IPC-6018, "Microwave End Product Board Inspection and Test" IPC A-600, "Guidelines for Acceptability of Printed Boards" * IPC-6011, IPC-6012, IPC-6013 must use Class 3 Requirements	
Place/Time/Purpose of Delivery: Prior to population of flight PWBs. Applies individually to each procured lot of boards.	
Preparation Information: Prior to population of PWBs: • Contact GSFC Materials Engineering Branch (MEB), Code 541. • Submit test coupons for destructive physical analysis (DPA) per Code 541 procedures. • Do not release PWBs for population until notification by MEB that test coupons passed DPA.	

Table 18-34. DID 11-1: Materials and Processes Control Program Plan

Title: Materials and Processes Control Program Plan	**CDRL Number:** 11-1
Reference: Section 11.1	
Use: Description of developers approach and methodology for implementing MPCP, including flow-down of applicable MPCP requirements to sub-developers.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: The MPCP shall be developed and delivered as part of the proposal for LRO Review	
Preparation Information: The MPCP shall address all M&P program requirements. The MPCP shall contain, at a minimum, detailed discussions of the following: a. The developer's plan or approach for conforming to M&P requirements. b. The developer's M&P control organization, identifying key individuals and specific responsibilities. c. M&P tracking methods and approach, including tools to be used such as databases, reports, etc. Describe system for identifying and tracking M&P approval status. d. M&P procurement, processing and testing methodology and strategies. Identify internal operating procedures to be used for incoming inspections, screening, qualification testing, derating, testing of M&P pulled from stores, DPA, radiation assessments, etc. e. M&P vendor surveillance and audit plan. f. Electrostatic Control Plan g. Flow-down of MPCP requirements to sub-developers. h. May be part of the developer/contractor Assurance Implementation Plan	

Table 18-35. DID 11-2: As-Designed Materials and Processes List

Title: As-Designed Materials and Processes List	**CDRL Number:** 11-2
Reference: Section 11.2	
Use: Listing of Materials and Processes intended for use in space flight hardware.	
Related Documents: Materials and Processes Control Program Plan, DIDs 11-5, 11-7, 11-9, 11-11	
Place/Time/Purpose of Delivery: Submission to LRO 30 days prior to PDR and CDR. Updates as required, including changes.	
Preparation Information: The As-Designed Materials and Processes List (ADMPL) shall be compiled by instrument, instrument component, or SC component, and shall include the following information at a minimum: a. Materials and Processes name b. Materials and Processes number c. Manufacturer d. Manufacturer's generic Materials and Processes number e. Procurement specification Any format may be used, provided the required information is included. All submissions to LRO will include a paper copy and a computer readable form.	

Table 18-36. DID 11-3: Materials Usage Agreement

Title: Materials Usage Agreement	**CDRL Number:** 11-3
Reference: Section 11.2	
Use: For usage evaluation and approval of non-compliant materials or lubrication use.	
Related Documents: MSFC-STD-3029 MSFC-HDBK-527 AFSCM 91-710 NASA-STD-6001	
Place/Time/Purpose of Delivery: Provide to the LRO, with the Polymeric Materials List, flammable materials usage list, odor and toxic offgassing materials usage list, or the Inorganic Materials List for approval.	
Preparation Information: A Materials Usage Agreement (MUA) shall be provided for each non-compliant off-the-shelf hardware material usage, non-compliant polymeric material outgassing, flammability or toxicity usage, and non-compliant inorganic material stress corrosion cracking usage. The MUA shall be provided on a MUA form, a developer's equivalent form, or the developer's electronically transmitted form. The form is available in the Mission Assurance Guide. The MUA form requires the minimum following information: MSFC-STD-3029 material rating, usage agreement number, page number, drawing numbers, part or drawing name, assembly, material name and specification, manufacturer and trade name, use thickness, weight, exposed area, pressure, temperature, exposed media, application, rationale for safe and successful flight, originator's name, project manager's name, and date. The off-the-shelf hardware usage shall identify the measures to be used to ensure the acceptability of the hardware, such as hermetic sealing, material changes to known compliant materials, and vacuum bake-out to the error budget requirements listed in the CCP.	

Table 18-37. DID 11-4: Stress Corrosion Evaluation Form

Title: Stress Corrosion Evaluation Form	**CDRL Number:** 11-4
Reference: Section 11.2	
Use: Provide detailed SCC engineering information required to demonstrate the successful flight of the material usage.	
Related Documents: MSFC-STD-3029 AFSCM 91-710	
Place/Time/Purpose of Delivery: Provide to the LRO with the DIDs 11-3 and 11-4 for approval.	
Preparation Information: The developer shall provide the information requested on the stress corrosion evaluation form, the equivalent information on the developer's form or the equivalent information electronically. The form is available in the Mission Assurance Guide. The stress corrosion evaluation form requires, at a minimum, the following information: part number, part name, next assembly number, manufacturer, material heat treatment, size and form, sustained tensile stresses, magnitude and direction, process residual stress, assembly stress, design stress, static stress, special processing, weld alloy form, temper of parent weldment metal, weld filler alloy, welding process, weld bead removal if any, post-weld thermal treatment, post-weld stress relief, environment, protective finish, function of part, effect of failure, evaluation of stress corrosion susceptibility.	

Table 18-38. DID 11-5: Polymeric Materials List

Title: Polymeric Materials List	**CDRL Number:** 11-5
Reference: Section 11.2.1	
Use: For usage evaluation and approval of all polymeric and composite materials applications.	
Related Documents: NASA RP-1124 ASTM E 595 MSFC-HDBK-527 AFSCM 91-710, "Range Safety User Requirements Manual" GMI 1700.3 NASA-STD-6001	
Place/Time/Purpose of Delivery: Provide 30 days before PDR for LRO review. 60 days before CDR for LRO approval. 30 days before acceptance for LRO approval.	
Preparation Information: The developer shall provide the information requested on the Polymeric Materials List form, the equivalent information on the developer's form, or the equivalent information electronically. The form is available in the Mission Assurance Guide. The Polymeric Materials List[1] form requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer, address, prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, date evaluated, item number, material identification[2], mix formula[3], cure[4], amount code, expected environment[5], outgassing values, and reason for selection[6]. Notes 1 through 6 are listed below. 1. List all polymeric materials and composites applications used in the system, except lubricants that should be listed on the polymeric and composite materials usage list. 2. Give the name of the material, identifying number, and manufacturer. Example: Epoxy, Epon 828, E.V. Roberts and Associates 3. Provide Proportions and name of resin, hardener (catalyst), filler, etc. Example: 828/V140/Silflake 135 as 5/5/38 by weight 4. Provide cure cycle details. Example: 8 hrs at room temperature + 2 hrs at 150°C 5. Provide the details of the environment that the material will experience as a finished SC component, both in ground test and in space. List all materials with the same environment in one group. Example: T/V: -20C/+60C, 2 weeks, 10E-5torr, ultraviolet radiation (UV) Storage: up to one year at room temperature Space: -10C/+20C, 2 years, 150 mile altitude, UV, electron, proton, atomic oxygen 6. Provide any special reason why the materials were selected. If for a particular property, please list property. Example: Cost, availability, room temperature curing, or low thermal expansion.	

Table 18-39. DID 11-6: Waiver

Title: Materials Waiver	**CDRL Number:** 11-6
Reference: Section 11.5	
Use: For usage evaluation and approval of a material that has exceeded its shelf life or expiration date.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Provide to the LRO Office for approval 15 days prior to use.	
Preparation Information: A waiver shall be submitted for approval of uncured polymers that have exceeded their expiration date or for flight approval of cured polymers and lubricated mechanisms that have a limited shelf life. For uncured polymers, data must be submitted to demonstrate that the cured paint or polymer is acceptable. This data may either be mechanical and physical properties from the same batch of expired uncured materials, or test data on identical expired uncured polymers or paints. For lubricated mechanisms and old polymer products such and o-rings, propellant tank diaphragms, seals dampers and tapes, mechanical and physical property data, test results and heritage performance information shall be submitted to demonstrate the flight acceptability of the hardware.	

Table 18-40. DID 11-7: Inorganic Materials List

Title: Inorganic Materials List	**CDRL Number:** 11-7
Reference: Paragraph 11.2.2	
Use: For usage evaluation and approval of all metal, ceramic, and metal/ceramic composite material applications.	
Related Documents: MSFC-HDBK-527 AFSCM 91-710 MSFC-STD-3029	
Place/Time/Purpose of Delivery: 30 days before the PDR for LRO review. 30 days before CDR for LRO approval. 30 days prior to acceptance for approval.	
Preparation Information: The hardware provider shall provide the information requested on the Inorganic Materials List, the equivalent information on the hardware developer's forms or the equivalent information electronically. The Inorganic Materials List [1] form requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer (and address), prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, item number, materials identification[2], condition[3], application or usage[4], expected environment[5], stress corrosion cracking table number, MUA number and NDE method. Notes 1 through 5 are listed below: 1. List all inorganic materials (metals, ceramics, glasses, liquids and metal/ceramic composites) except bearing and lubrication materials that should be listed on Form 18-59C. 2. Give materials name, identifying number manufacturer. Example: a. Aluminum 6061-T6 b. Electroless nickel plate, Enplate Ni 410, Enthone, Inc c. Fused silica, Corning 7940, Corning Class Works 3. Give details of the finished condition of the material, heat treat designation (hardness or strength), surface finish and coating, cold worked state, welding, brazing, etc. Example: a. Heat-treated to Rockwell C 60 hardness, gold electroplated, brazed. b. Surface coated with vapor deposited aluminum and magnesium fluoride c. Cold worked to full hare condition, TIG welded and electroless nickel-plated. 4. Give details of where on the SC the material shall be used (component) and its function. Example: Electronics box structure in attitude control system, not hermetically sealed. 5. Give the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. Exclude vibration environment. List all materials with the same environment in one group. Example: a. T/V: -20C/+60C, 2 weeks, 10E-5 torr, Ultraviolet radiation (UV) b. Storage: up to 1 year at room temperature c. Space: -10C/+20C, 2 years, 150 miles altitude, UV, electron, proton, Atomic Oxygen	

Table 18-41. DID 11-8: Fastener Control Plan

Title: Fastener Control Plan	**CDRL Number:** 11-8
Reference: Section 11.2.5	
Use: For LRO evaluation and approval.	
Related Documents: 541-PG-8072.1.2 AFSCM 91-710 GSFC 731-0005-83 GMI 1700.3	
Place/Time/Purpose of Delivery: With proposal for LRO review. 30 days before the PDR for LRO approval.	
Preparation Information: The developer's fastener control plan shall address the following for flight hardware threaded fasteners that are used in structural or critical applications: a. Acquisition/supplier control b. Documentation/traceability c. Receiving inspection/testing	

Table 18-42. DID 11-9: Lubrication Materials List

Title: Lubrication Materials List	**CDRL Number:** 11-9
Reference: Section 11.2.3	
Use: For evaluation and approval of all lubricant usage and applications.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: 30 days before the PDR for LRO review. 30 days before CDR for LRO approval. 30 days prior to acceptance for approval.	
Preparation Information: The hardware provider shall provide the information requested on the Lubrication Materials List form, the equivalent information on the hardware developer's forms, or the equivalent information electronically. The form is available in the Mission Assurance Guide. The Lubrication Materials List form requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer (and address), prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, item number, component type, size, material[1]; component manufacturer and manufacturer identification; proposed lubrication system and amount of lubrication; type and number of wear cycles[2]; speed, temperature, and atmosphere of operation[3]; type and magnitude of loads[4]; and other details[5]. Notes 1 through 5 are listed below: 1. For ball bearings (BB), sleeve bearings (SB), gears (G), sliding surfaces (SS), and sliding electrical contacts (SEC) give generic identification of materials used for the component. Example: 440C steel, PTFE 2. Types of wear cycles: continuous unidirectional rotation (CUR), continuous operation (CO), intermittent rotation (IR), intermittent oscillation (IO), small angle oscillation (<30 degrees) (SAO), large angle oscillation (>30degrees) (LAO), continuous sliding (CS), intermittent sliding (IS). Number of wear cycles: 1 to 1E2 (A), 1E2 to 1E4 (B), 1E4 to 1E6 (C), >1E6 (D). 3. Speed: revolution per min. (RPM), oscillation per min. (OPM), variable speed (VS), sliding speed in cm per min. (CPM); Operational Temperature Range; Atmosphere: vacuum, air, gas sealed or unsealed, and pressure 4. Type of loads: Axial, radial, tangential (gear load). Give magnitude of load. 5. For ball bearings, give type and material of ball cage, number of shields, type of ball grove surface finishes. For gears, give surface treatment and hardness. For sleeve bearings, give the bore diameter and width. Provide the torque and torque margins.	

Table 18-43. DID 11-10: Life Test Plan for Lubricate Mechanisms

Title: Life Test Plan for Lubricated Mechanisms	**CDRL Number:** 11-10
Reference: Section 11.2.3	
Use: For evaluation and approval of all lubricated mechanisms.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: 30 days before the PDR for LRO review. 30 days before CDR for LRO approval. 30 days prior to acceptance for approval.	
Preparation Information: The Life Test Plan for Lubricated Mechanisms shall contain: a. Table of Contents. b. Description of all lubricated mechanisms, performance functions, summary of subsystem specifications, and life requirements. c. Heritage of identical mechanisms and descriptions of identical applications. d. Design, drawings, and lubrication system used by the mechanism. e. Test plan, including vacuum, temperature, and vibration test environmental conditions. f. Criteria for a successful test. g. Delivery of test hardware to GSFC after a successful test. h. Final report.	

Table 18-44. DID 11-11: Material Processes List

Title: Material Processes List	**CDRL Number:** 11-11
Reference: Paragraph 11.2.4	
Use: For usage evaluation and approval of all material processes used to fabricate, clean, store, integrate and test the space flight hardware.	
Related Documents: 431-RQMT-000174, "LRO Mission Assurance Requirements"	
Place/Time/Purpose of Delivery: 30 days before the PDR for LRO review. 30 days before CDR for LRO approval. 30 days prior to acceptance for approval. A copy of any process shall be submitted to the LRO Office upon request.	
Preparation Information: The provider shall provide the information requested on the Material Processes List form, the equivalent information on the developer's forms, or the equivalent information electronically. The form is available in the Mission Assurance Guide. The material process utilization list requires, at a minimum, the following information: SC, subsystem or instrument name, GSFC technical officer, developer (and address), prepared by (and phone number), date of preparation, GSFC materials evaluator (and phone number), date received, date evaluated, item number, process type[1], developer specification number[2]; military, ASTM, federal, or other specification number; description of material processed[3], and SC/instrument application[4]. Notes 1 through 4 are listed below: 1. Give generic name of the process. Example: anodizing (sulfuric acid) 2. Please state such if process is proprietary. 3. Identify the type and condition of the material subjected to the process. Example: 6061-T6 4. Identify the component or structure for which the materials are being processed. Example: Antenna dish All welding and brazing of all flight hardware, including repairs, shall be performed by certified operators, in accordance with requirements of the appropriate industry or government standards listed in the Materials Process Utilization List (LRO MAR, Figure 11-6). A copy of the procedure qualification record (PQR) and a current copy of the operator qualification test record shall be provided along with the Material Processes List.	

Table 18-45. DID 11-12: Certificate of Raw Material Compliance

Title: Certificate of Raw Material Compliance	**CDRL Number:** 11-12
Reference: Section 11.4	
Use: For information assuring acceptable flaw content, chemical composition, and physical properties of raw material.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: Provide LRO within 15 days of request.	
Preparation Information: The provider shall provide information pertaining to the control of raw material. The developer shall provide sufficient information to ensure that the supplied material meets the specified requirements. The developer shall indicate the SC and subsystem/instrument and part using the material. The generic and manufacturer's designation (if any) shall be provided for the material, including the type of test employed to verify material composition. The provider shall indicate what tests have been performed to verify physical properties and the applicable standards controlling the testing. For example, the heat treated condition of aluminum alloys may be verified by mechanical testing or harness and conductivity testing. The provider shall indicate what nondestructive tests have been performed, the applicable standards controlling the testing, the types of flaws detected, and the minimum detectable flaw found as a result of the testing.	

Table 18-46. DID 12-1 Parts Control Plan (PCP)

Title: Parts Control Plan	**CDRL Number:** 12-1
Reference: Section 12.1	
Use: Description of developer's approach and methodology for implementation of the Parts Control Program.	
Related Documents: Parts Identification List (PIL)	
Place/Time/Purpose of Delivery: Developed and delivered with, or incorporated into, the developer's Performance Assurance Implementation Plan for GSFC review. It will be delivered for GSFC approval. Subsequent revisions will be delivered for GSFC approval.	
Preparation Information: The PCP will address all EEE parts program requirements. The PCP will contain, at a minimum, detailed discussions of the following: a. The developer's plan or approach for conforming to the EEE parts requirements. b. The developer's parts control organization, identifying key individuals, and specific responsibilities. c. Detailed PCB procedures, to include membership, designation of Chairperson, responsibilities, review and approval procedures, meeting schedules and notification method, meeting minutes, etc. d. Parts tracking methods and approach, including tools to be used such as databases, reports, PIL, etc. Description of the system for identifying and tracking parts approval status. e. Parts procurement, processing and testing methodology and strategies. Identify internal operating procedures to be used for incoming inspections, screening, qualification testing, derating, testing of parts pulled form stores, DPA, radiation assessments, etc.	

Table 18-47. DID 12-2 Parts Control Board (PCB) Reports

Title: Parts Control Board Reports	**CDRL Number:** 12-2
Reference: Section 12.2.2	
Use: Document all Parts Control Board (PCB) meetings	
Related Documents: Parts Control Plan	
Place/Time/Purpose of Delivery: PCB Reports will be submitted to GSFC for review within five workdays of each PCB meeting.	
Preparation Information: Actions and recommendations from reviews and discussions of all issues affecting EEE parts (e.g., alert finding, DPA results, failure analysis results, qualification basis, screening requirements, etc.) shall be recorded in the PCB reports.	

Table 18-48. DID 12-3 Parts Identification List (PIL)

Title: Parts Identification List	**CDRL Number:** 12-3
Reference: Sections 12.6.1, 12.6.2, 12.6.3	
Use: Listing of all EEE parts intended for use in spaceflight hardware.	
Related Documents: Parts Control Plan	
Place/Time/Purpose of Delivery: 30 days before PDR for GSFC approval. Subsequent revisions, with changes clearly noted, for GSFC approval. Updated revision 30 days before CDR for GSFC approval. The As-Built Parts List (ABPL) will be developed from this document/database, and will be submitted to GSFC for review 60 days prior to delivery of the end item.	
Preparation Information: The PIL/PPL/ABPL will be prepared and maintained throughout the life of the project. They will be compiled by the instrument developer or instrument component developer, and will include the following information at a minimum: a. Part name b. Part number c. Manufacturer d. Manufacturer's generic part number e. Procurement specification f. GIDEP Alert status Any format may be used, provided the required information is included. All submissions to GSFC will be provided in an electronic spreadsheet format, with changes from the last revision shall be clearly noted (identified with date and revision level). Note: The ABPL will include the following information in addition to the above list: a. Lot date code b. Quantities c. Parts use location to the sub-assembly level or reference designator	

Table 18-49. DID 12-4 Alert / Advisory Disposition and Preparation

Title: Alert/Advisory Disposition and Preparation	**CDRL Number:** 12-4
Reference: Section 12.5.3	
Use: Review the disposition of GIDEP Alerts and NASA Alerts and Advisories (provided to the Developer by GSFC or another source). Prepare, or assist GSFC in preparing, Alerts/Advisories based on part anomalies/concerns resulting from the Developer's experience.	
Related Documents: Parts Control Plan	
Place/Time/Purpose of Delivery: Response to GSFC within 25 days or Alert/Advisory receipt. Alert/Advisory impacts, if any, should be discussed at technical reviews and PCB meetings. This information will be provided to GSFC for information, and concurrence that all flight hardware is flight worthy. Developer-prepared alerts/advisories will be prepared within 60 days in coordination with GSFC, as needed.	
Preparation Information: The developer will provide an impact statement to GSFC for each Alert/Advisory reviewed. When a negative impact exists, the developer will provide a narrative plan of action and an implementation date within 25 calendar days of Alert/Advisory receipt. The developer will notify GSFC within two work days of discovering a suspect part/lot. Information will be shared with GSFC to enable GSFC cooperation in the preparation of the Alert/Advisory (if necessary).	

Table 18-50. DID 13-1: Contamination Control Plan

Title: Contamination Control Plan	**CDRL Number:** 13-1
Reference: Section 13.1	
Use: To establish contamination allowances and methods for controlling contamination.	
Related Documents: N/A	
Place/Time/Purpose of Delivery: 30 days before PDR for GSFC review, 30 days before CDR for GSFC approval.	
Preparation Information: Data on material properties, design features, test data, system tolerance of degraded performance, and methods to prevent degradation shall be provided to permit independent evaluation of contamination hazards. The following items should be included in the plan: 1. Materials a. Outgassing as a function of temperature and time. b. Nature of outgassing chemistry. c. Areas, weight, location, and view factors of critical surfaces. 2. Venting: size, location, and relation to external surfaces. 3. Thermal vacuum test contamination monitoring plan, including vacuum test data, QCM location and temperature, pressure data, system temperature profile and shroud temperature. 4. On-orbit SC and instrument performance as affected by contamination deposits. a. Contamination effect monitor. b. Methods to prevent and recover from contamination in orbit. c. How to evaluate on-orbit degradation. d. Photopolymerization of outgassing products on critical surfaces. e. Space debris risks and protection. f. Atomic oxygen erosion and re-deposition. 5. Analysis of contamination impact on the satellite on-orbit performance. 6. On-orbit contamination impact from other sources, such as STS, space station, and adjacent instruments.	

Table 18-51. DID 14-1: Electrostatic Discharge Control Plan

Title: Electrostatic Discharge Control Plan	**CDRL Number:** 14-1
Reference: Section 14.1	
Use: To establish ESD controls for manufacturing and handling sensitive flight hardware.	
Related Documents: ANSI/ESD S20.20, "Association Standard for the Development of an Electrostatic Control Program for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (excluding electrically initiated explosive devices)"	
Place/Time/Purpose of Delivery: 30 days before PDR for GSFC review, 30 days before CDR for GSFC approval.	
Preparation Information: The developer shall document the requirements of ANSI/ESD S20.20 will be met for the life of the project. The developer shall document any ESD event which violates the ESD program, and notify GSFC of the event and corrective action per the PFR or problem reporting system, as defined in the quality or mission assurance plan.	

Table 18-52. DID 16-1: End Item Data Package

Title: End Item Data Package	**CDRL Number:** 16-1
Reference: Section 16.0	
Use: Contains all reports on as-built and tested flight hardware to be delivered to the LRO Project	
Related Documents: N/A	
Place/Time/Purpose of Delivery: At PSR for GSFC approval	
Preparation Information: The end item data package shall contain at a minimum the following: • Acceptance Testing (as-run) procedures and reports including total number of failure free testing • Environmental testing (as-run) reports • Final Assembly Work Order • Material Certification or Analysis Forms • Waivers, Deviations or MUAs • As-Built EEE parts list • As-Built materials List (ABML) • End Item Inspection Report • Nonconformance or problem/failure reports and corrective action summaries • List of Open items or one time occurrences • As-Built final assembly drawing • Any pertinent analyses (mechanical, electrical, reliability, stress, thermal, worst-case) • As-Built configuration list (Item, Manufacturer, Model, etc.) • Certification of Compliance signed by management	

Appendix A. Abbreviations and Acronyms

Abbreviation/ Acronym	DEFINITION
ABPL	As-Built Parts List
ABML	As-Built Materials List
ADMPL	As-Designed Materials and Processes List
AFSPC	Air Force Space Command
ANSI	American National Standards Institute
AR	Acceptance Review
ASIC	Application Specific Integrated Circuits
ASQ	American Society for Quality
ASQC	American Society for Quality Control
ASTM	American Society for Testing of Materials
BB	Ball Bearing
BGA	Ball Grid Array
C	Centigrade
CAGE	Commercial and Government Entity
CCB	Configuration Control Board
CCP	Contamination Control Plan
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Delivery Requirements List
CFR	Code of Federal Regulations
CIL	Critical Items List
CM	Configuration Management
CMO	Configuration Management Office
CO	Continuous Oscillation
COB	Chip on Board
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-the-Shelf
CPM	Centimeters per minute
CRM	Continuous Risk Management
CRMS	Continuous Risk Management System
CS	Continuous Sliding
CSCI	Computer Software Configuration Item
CUR	Continuous Unidirectional Rotation
CVCM	Collected Volatile Condensable Mass
DID	Data Item Description
DoD	Department of Defense
DOORS	Dynamic Object Oriented Requirements System

Abbreviation/ Acronym	DEFINITION
DPA	Destructive Physical Analysis
DSCC	Defense Supply Center Columbus
EEE	Electrical, Electronic, and Electromechanical
EIA	Electronics Industry Alliance
EIDP	End Item Data Package
EIS	Environmental Impact Statement
ELDR	Enhanced Low Dose Rate
ELV	Expendable Launch Vehicle
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ESMD	Exploration Systems Mission Directorate
ETA	Event Tree Analysis
ETM	Environmental Test Matrix
ETR	Eastern Test Range
EVA	Extravehicular Activity
EWR	Eastern and Western Test Ranges
FA	Failure Analysis
FAP	Flight Assurance Procedure
FAR	Federal Acquisition Regulations
FCA	Functional Configuration Audit
FETs	Field Effect Transistors
FMEA	Failure Modes and Effects Analysis
FOR	Flight Operations Review
FRB	Failure Review Board
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
FY	Fiscal Year
G	Gears
GDS	Ground Data System
GEVS	General Environmental Verification Standards
GFE	Government-Furnished Equipment
GHB	Goddard Space Flight Center Handbook
GIA	Government Inspection Agency
GIDEP	Government Industry Data Exchange Program
GMI	Goddard Management Instruction
GOTS	Government Off-the-Shelf
GPMC	Governing Program Management Council

Abbreviation/ Acronym	DEFINITION
GPR	Goddard Procedure and Guidelines
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
hrs	hours
HTL	Hazard Tracking Log
HQ	Headquarters
I&T	Integration and Test
IAC	Independent Assurance Contractor
IEEE	Institute of Electrical and Electronics Engineers
IIR	Integrated Independent Review
IIRT	Integrated Independent Review Team
INST	Instruction
IO	Intermittent Oscillation
IPC	Association Connecting Electronics Industries
IR	Intermittent Rotation
IS	Intermittent Sliding
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
JSC	Johnson Space Center
KHB	Kennedy Space Center Handbook
KSC	Kennedy Space Center
LAO	Large Angle Oscillation
LRO	Lunar Reconnaissance Orbiter
LRU	Line Replaceable Unit
M	Million
M&P	Materials and Processes
M&PCP	Materials and Processes Control Program
MAE	Materials Assurance Engineer
MAG	Mission Assurance Guidelines
MCM	Multi-Chip Module
MEB	Materials Engineering Branch
MIL	Materials Identification List
MLD	Master Logic Diagram
mm	millimeter
MOR	Mission Operations Review
MOSFETs	Metal-Oxide-Semiconductor Field Effect Transistors
MOTS	Modified Off-the-Shelf
MPCP	Materials and Processes Control Plan

Abbreviation/ Acronym	DEFINITION
MRB	Materials Review Board
MRR	Mission Readiness Review
MSFC	Marshall Space Flight Center
MSPSP	Missile System Pre-Launch Safety Data Package
MSR	Monthly Status Review
MUA	Materials Usage Agreement
NASA	National Aeronautics and Space Administration
NCR	Nonconformance Report
NHB	NASA Handbook
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NPSL	NASA Parts Selection List
NSF	NASA Federal Supplement
NSPAR	Nonstandard Parts Approval Request
NSS	NASA Safety Standard
O_2	Oxygen
O&SHA	Operating and Support Hazard Analysis
ODA	Orbital Debris Assessment
OHA	Operational Hazard Analysis
OPM	Oscillation per minute
OSSMA	Office of Systems Safety and Mission Assurance
PAPL	Project Approved Parts List
PCA	Physical Configuration Audit
PCB	Parts Control Board
PCP	Parts Control Plan
PDA	Percentage of Defective Allowable
PDR	Preliminary Design Review
PEM	Plastic Encapsulated Microcircuit
PER	Pre-Environmental Review
PFR	Problem/Failure Report
PG	Procedures and Guidelines
PHA	Preliminary Hazards Analysis
PIL	Parts Identification List
PIND	Particle Impact Noise Detection
POCC	Payload Operations Control Center
PPE	Project Parts Engineer
PPL	Preferred Parts List
PQR	Procedure Qualification Record

Abbreviation/ Acronym	DEFINITION
PRA	Probabilistic Risk Assessment
PRE	Project Radiation Engineer
PSM	Project Safety Manager
PSR	Pre-Shipment Review
PSSSMA	Performance Specification Sheet for Space and Military Avionics
PTFE	Polytetrafluoroethylene
PWB	Printed Wiring Board
PWQ	Process Waste Questionnaire
QA	Quality Assurance
QCM	Quartz Crystal Microbalance
QMS	Quality Management System
R&M	Reliability and Maintainability
RBAM	Risk-Based Acquisition Management
RDM	Radiation Design Margin
RF	Radio Frequency
RFA	Request for Action
RLAT	Radiation Lot Acceptance Test
RMP	Risk Management Plan
RPP	Reliability Program Plan
RPM	Revolutions Per Minute
RVM	Requirements Verification matrix
SAE	Society of Automotive Engineers
SAM	System Assurance Manager
SAO	Small Angle Oscillation
SAR	Safety Assessment Report
SB	Sleeve Bearings
SC	Spacecraft
SCC	Stress Corrosion Cracking
SCM	Software Configuration Management
SCR	System Concept Review
SEB	Single-Event Burn-Out
SEC	Sliding Electrical Contacts
SEGR	Single-Event Gate Rupture
SEE	Single-Even Effects
SEL	Single-Event Latch up
SEM	Scanning Electronic Microscope
SET	Single-Event Transient
SEU	Single-Event Upset

Abbreviation/ Acronym	DEFINITION
SHA	System Hazard Analysis
SMA	Safety and Mission Assurance
SOW	Statement of Work
SRO	Systems Review Office
SRP	System Review Program
SRR	System Requirements Review
SS	Sliding Surface
SSHA	Subsystem Safety Hazard Analysis
SSPP	System Safety Program Plan
STD	Standard
STS	Space Transportation System
STT	Strategy-to-Task-to-Technology
SWG	Safety Working Group
SWRR	Software Requirements Review
TID	Total Ionizing Dose
TIG	tungsten inert gas
TIM	Technical Interface Meeting
TML	Total Mass Loss
TRR	Test Readiness Review
U.S.	United States
UV	Ultraviolet
V&V	Verification and Validation
VDD	Version Description Document
VTL	Verification Tracking Log
WOA	Work Order Authorization

Appendix B. Glossary/Definitions

The following definitions apply within the context of this document:

Acceptance Tests: The validation process that demonstrates that hardware is acceptable for flight. It also serves as a quality control screen to detect deficiencies and, normally, to provide the basis for delivery of an item under terms of a contract.

Assembly: See Level of Assembly.

Audit: A review of the developer's or sub-developer's documentation or hardware to verify that it complies with project requirements.

Collected Volatile Condensable Material (CVCM): The quantity of outgassed matter from a test specimen that condenses on a collector maintained at a specific constant temperature for a specified time.

Component: See Level of Assembly.

Configuration: The functional and physical characteristics of the payload and all its integral parts, assemblies, and systems capable of fulfilling the fit, form and functional requirements defined by performance specifications and engineering drawings.

Configuration Control: The systematic evaluation, coordination, and formal approval/disapproval of proposed changes, including the implementation of all approved changes to the design and production of an item with a configuration formally approved by the developer/purchaser/both.

Configuration Management (CM): The systematic control and evaluation of all changes to baseline documentation and subsequent changes to that documentation which define the original scope of effort to be accomplished (contract and reference documentation) and the systematic control, identification, status accounting and verification of all configuration items.

Contamination: The presence of materials of molecular or particulate nature, which degrade the performance of hardware.

Derating: The reduction of the applied load (or rating) of a device to improve reliability or to permit operation at high ambient temperatures.

Design Specification: Generic designation for a specification that describes functional and physical requirements for an article, usually at the component level or higher levels of assembly. In its initial form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements.

The design specification evolves through the project life cycle to reflect progressive refinements in performance, design, configuration, and test requirements. In many projects, the end-item

specifications serve all the purposes of design specifications for the contract end-items. Design specifications provide the basis for technical and engineering management control.

Designated Representative: An individual (such as a NASA plant representative), firm (such as assessment developer), Department of Defense (DoD) plant representative, or other government representative designated and authorized by NASA to perform a specific function for NASA. As related to the developer's effort, this may include evaluation, assessment, design review, participation, and review/approval of certain documents or actions.

Destructive Physical Analysis (DPA): An internal destructive examination of a finished part or device to assess design, workmanship, assembly, and any other processing associated with fabrication of the part.

Design Qualification Tests: Tests intended to demonstrate that an item will function within performance specifications under simulated conditions more severe than those expected from ground handling, launch, and orbital operations. Their purpose is to uncover deficiencies in design and method of manufacture. They are not intended to exceed design safety margins or to introduce unrealistic modes of failure. The design qualification tests may be to either "prototype" or "protoflight" test levels.

Discrepancy: See Nonconformance.

Electromagnetic Compatibility (EMC): The condition that prevails when various electronic devices are performing their functions according to design in a common electromagnetic environment.

Electromagnetic Interference (EMI): Electromagnetic energy, which interrupts, obstructs, or otherwise degrades or limits the effective performance of electrical equipment.

Electromagnetic Susceptibility: Undesired response by a component, subsystem, or system to conducted or radiated electromagnetic emissions.

End-to-End Tests: Tests performed on the integrated ground and flight system, including all elements of the payload, its control, stimulation, communications, and data processing to demonstrate that the entire system is operating in a manner to fulfill all mission requirements and objectives.

Failure: A departure from specification that is discovered in the functioning or operation of the hardware or software. See nonconformance.

Failure Modes and Effects Analysis (FMEA): A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed to determine the effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

Flight Acceptance: See Acceptance Tests.

Fracture Control Program: A systematic project activity to ensure that a payload intended for flight has sufficient structural integrity as to present no critical or catastrophic hazard. Also, to ensure quality of performance in the structural area for any payload (SC) project. Central to the program is fracture control analysis, which includes the concepts of fail-safe and safe-life, defined as follows:

a. *Fail-safe:* Ensures that a structural element, because of structural redundancy, will not cause collapse of the remaining structure or have any detrimental effects on mission performance.

b. *Safe-life:* Ensures that the largest flaw that could remain undetected after non-destructive examination would not grow to failure during the mission.

Functional Tests: The operation of a unit in accordance with a defined operational procedure to determine whether performance is within the specified requirements.

Hardware: As used in this document, there are two major categories of hardware as follows:

a. *Prototype Hardware:* Hardware of a new design; it is subject to a design qualification test program and is not intended for flight.

b. *Flight Hardware:* Hardware to be used operationally in space. It includes the following subsets:

(i) Protoflight Hardware: Flight hardware of a new design, subject to a qualification test program that combines elements of prototype and flight acceptance verification; that is, the application of design qualification test levels and duration of flight acceptance tests.

(ii) Follow-On Hardware: Flight hardware built in accordance with a design that has been qualified either as prototype or as protoflight hardware; follow-on hardware is subject to a flight acceptance test program.

(iii) Spare Hardware: Hardware whose design has been proven in a design qualification test program, subject to a flight acceptance test program and used to replace flight hardware that is no longer acceptable for flight.

(iv) Re-flight Hardware: Flight hardware that has been used operationally in space and is to be reused in the same way; the validation program to which it is subject depends on its past performance, current status, and the upcoming mission.

Inspection: The process of measuring, examining, gauging, or otherwise comparing an article or service with specified requirements.

Instrument: See Level of Assembly.

Level of Assembly: The environmental test requirements of GEVS generally start at the component or unit-level assembly and continue hardware/software build through the system level (referred to in GEVS as the payload or SC level). The assurance program includes the part level. Verification testing may also include testing at the assembly and subassembly levels of assembly; for test recordkeeping these levels are combined into a "subassembly" level. The verification program continues through launch, and on-orbit performance. The following levels of assembly are used for describing test and analysis configurations:

a. *Part:* A hardware element that is not normally subject to further subdivision or disassembly without destruction of design use. Examples include resistor, integrated circuit, relay, connector, bolt, and gaskets.

b. *Subassembly:* A subdivision of an assembly. Examples are wire harness and loaded printed circuit boards.

c. *Assembly:* A functional subdivision of a component consisting of parts or subassemblies that perform functions necessary for the operation of the component as a whole. Examples are a power amplifier and gyroscope.

d. *Component or unit:* A functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem's operation. Examples are electronic box, transmitter, gyro package, actuator, motor, battery. For the purposes of this document, "component" and "unit" are used interchangeably.

e. *Section:* A structurally integrated set of components and integrating hardware that form a subdivision of a subsystem, module, etc. A section forms a testable level of assembly, such as components/units mounted into a structural mounting tray or panel-like assembly, or components that are stacked.

f. *Subsystem:* A functional subdivision of a payload consisting of two or more components. Examples are structural, attitude control, electrical power, and communication subsystems. Also included as subsystems of the payload are the science instruments or experiments.

g. *Instrument*: A SC subsystem consisting of sensors and associated hardware for making measurements or observations in space. For the purposes of this document, an instrument is considered a subsystem (of the SC).

h. *Module:* A major subdivision of the payload that is viewed as a physical and functional entity for the purposes of analysis, manufacturing, testing, and record keeping. Examples include SC bus, science payload and upper stage vehicle.

i. *Payload:* An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space. For the purposes of this document, "payload" and

"spacecraft" are used interchangeably. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

j. *Spacecraft:* See Payload. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

Limit Level: The maximum expected flight.

Limited Life Items: Spaceflight hardware that (1) has an expected failure-free life that is less than the projected mission life, when considering cumulative ground operation, storage and on-orbit operation, and (2) has limited shelf life material used to fabricate flight hardware.

Maintainability: A measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is characteristic of equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

Margin: The amount by which hardware capability exceeds mission requirements.

Mission Assurance: The integrated use of the tasks of system safety, reliability assurance engineering, maintainability engineering, mission environmental engineering, materials and processes engineering, electronic parts engineering, quality assurance, software assurance, configuration management, and risk management to support NASA projects.

Module: See Level of Assembly.

Monitor: To keep track of the progress of a performance assurance activity; the monitor need not be present at the scene during the entire course of the activity, but will review resulting data or other associated documentation (see Witness).

Nonconformance: A condition of any hardware, software, material, or service in which one or more characteristics do not conform to requirements. As applied in quality assurance, nonconformances fall into two categories – discrepancies and failures. A discrepancy is a departure from specification that is detected during inspection or process control testing, etc., while the hardware or software is not functioning or operating. A failure is a departure from specification that is discovered in the functioning or operation of the hardware or software.

Offgassing: The emanation of volatile matter of any kind from materials into a manned pressurized volume.

Outgassing: The emanation of volatile materials under vacuum conditions resulting in a mass loss and/or material condensation on nearby surfaces.

Part: See Level of Assembly.

Payload: See Level of Assembly.

Performance Verification: Determination by test, analysis, or a combination of the two that the payload element can operate as intended in a particular mission; this includes being satisfied that the design of the payload or element has been qualified and that the particular item has been accepted as true to the design and ready for flight operations.

Protoflight Testing: See Hardware.

Prototype Testing: See Hardware.

Qualification: See Design Qualification Tests.

Red Tag/Green Tag: Physical tags affixed to flight hardware that mean: red (remove before flight) and green (enable before flight).

Redundancy (of design): The use of more than one independent means of accomplishing a given function.

Reliability: The probability that an item will perform its intended function for a specified interval under stated conditions.

Repair: A corrective maintenance action performed as a result of a failure so as to restore an item to operate within specified limits.

Rework: Return for completion of operations (complete to drawing). The article is to be reprocessed to conform to the original specifications or drawings.

Section: See Level of Assembly.

Similarity: Verification by: a procedure of comparing an item to a similar one that has been verified. Configuration, test data, application and environment should be evaluated. It should be determined that design differences are insignificant, environmental stress will not be greater in the new application, and that manufacturer and manufacturing methods are the same.

Single Point Failure: The failure of a single hardware element which would result in loss of mission objectives, hardware, or crew, as defined for the specific application or project for which a single point failure analysis is performed.

Spacecraft: See Level of Assembly.

Subassembly: See Level of Assembly.

Subsystem: See Level of Assembly.

Temperature Cycle: A transition from some initial temperature condition to temperature stabilization at one extreme and then to temperature stabilization at the opposite extreme, then returning to the initial temperature condition.

Temperature Stabilization: The condition that exists when the rate of change of temperatures has decreased to the point where the test item may be expected to remain within the specified test tolerance for the necessary duration or where further change is considered acceptable.

Thermal Balance Test: A test conducted to verify the adequacy of the thermal model, the adequacy of the thermal design, and the capability of the thermal control system to maintain thermal conditions within established mission limits.

Thermal-Vacuum Test: A test conducted to demonstrate the capability of the test item to operate satisfactorily in vacuum at temperatures based on those expected for the mission. The test, including the gradient shifts induced by cycling between temperature extremes, can also uncover latent defects in design, parts, and workmanship.

Torque Margin: Torque margin is equal to the torque ratio minus one.

Torque Ratio: Torque ratio is a measure of the degree to which the torque available to accomplish a mechanical function exceeds the torque required.

Total Mass Loss (TML): Total mass of material outgassed from a specimen that is maintained at a specified constant temperature and operating pressure for a specified time.

Unit: See Level of Assembly.

Validation: The process of evaluating software during, or at the end of, the software development process to determine whether it satisfies specified requirements.

Verification: The process of evaluating software to determine whether the products of a given development phase (or activity) satisfy the conditions imposed at the start of that phase (or activity).

Vibroacoustics: An environment induced by high-intensity acoustic noise associated with various segments of the flight profile; it manifests itself throughout the payload in the form of directly transmitted acoustic excitation and as structure-borne random vibration.

Workmanship Tests: Tests performed during the environmental verification program to verify adequate workmanship in the construction of a test item. It is often necessary to impose stresses beyond those predicted for the mission in order to uncover defects. Thus random vibration tests are conducted specifically to detect bad solder joints, loose or missing fasteners, improperly mounted parts, etc. Cycling between temperature extremes during thermal-vacuum testing and the presence of electromagnetic interference during EMC testing can also reveal the lack of proper construction and adequate workmanship.

Witness: A personal, on-the-scene observation of a performance assurance activity with the purpose of verifying compliance with project requirements (see Monitor).