

DRAFT

Landsat Data Continuity Mission (LDCM)

Mission Assurance Requirements

05/24/2006



**National Aeronautics and
Space Administration**

**Goddard Space Flight Center
Greenbelt, Maryland**

CM FOREWORD

This document is a Landsat Data Continuity Mission (LDCM) 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 LDCM 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:

LDCM Configuration Management Office
Mail Stop 427
Goddard Space Flight Center
Greenbelt, Maryland 20771

DRAFT

Signature Page

Prepared by:

Jack Ellis
Systems Assurance Manager
GSFC Code 303

Date

Approved by:

William Ochs
LDCM Project Manager
Code 427

Date

Richard Day
Director, Office of
Systems Safety and
Mission Assurance

Date

DRAFT

Landsat Data Continuity Mission Project

DOCUMENT CHANGE RECORD

REV LEVEL	DESCRIPTION OF CHANGE	APPROVED BY	DATE APPROVED
<p>DRAFT</p>			

TABLE OF CONTENTS

	<u>Page</u>
Chapter 1.0 Overall Requirements	1
1.1 General	1
1.2 Surveillance of the Developer	1
1.3 Applicable Documents	2
1.4 Acronyms and Glossary	2
Chapter 2.0 Quality Management System	3
2.1 General	3
2.2 Supplemental Quality Management System Requirements	3
2.2.1 Control of Nonconforming Product.....	3
2.2.2 Material Review Board.....	3
2.2.3 Reporting of Failures	4
2.2.4 Control of Monitoring and Measuring Devices	4
2.2.5 Flow-Down of Requirements	4
2.2.6 Configuration Management	4
2.3 GIDEP Alerts And Problem Advisories.....	4
Chapter 3.0 System Safety Requirements.....	6
3.1 General Requirements	6
3.2 Design Requirements	6
3.3 System Safety Program Plan (SSPP).....	6
3.3.1 Preliminary Hazard Analysis	7
3.3.2 Operations Hazard Analysis.....	7
3.4 Safety Requirements Compliance Checklist	7
3.5 Missile System Prelaunch Safety Package.....	7
3.5.1 Verification Tracking Log (VTL).....	8
3.5.2 Ground Operations Procedures	8
3.5.3 Safety Variance	8
3.6 Support for Safety Working Group Meetings	9
3.7 Mishap Reporting And Investigation.....	9
3.8 Orbital Debris Assessment	9
Chapter 4.0 Reliability and Probabilistic Risk Assessment	10
4.1 General Requirements	10
4.2 Probabilistic Risk Assessment.....	10
4.3 Reliability Analyses	11
4.3.1 Failure Modes and Effects Analysis and Critical Items List	11
4.3.2 Fault Tree Analysis.....	11
4.3.3 Parts Stress Analyses	12
4.3.4 Worst-Case Analyses.....	12
4.3.5 Numerical Assessments and Predictions	12
4.4 Limited-Life Items	13
4.5 Control of Sub-Developers and Suppliers.....	13

4.8	Reliability Analysis of Test Data.....	14
4.8.1	Trend Analyses.....	14
4.8.2	Analysis of Test Results.....	15
Chapter 5.0	Software Assurance Requirements.....	16
5.1	Software Assurance.....	16
5.2	Software Quality.....	16
5.3	Software Safety.....	17
5.4	Software Reliability.....	18
5.5	Verification and Validation.....	18
5.6	Independent Verification and Validation.....	18
5.7	GFE, Existing and Purchased Software.....	18
Chapter 6.0	Contamination Control.....	19
6.1	General Requirements.....	19
6.2	Contamination Control Plan.....	19
6.3	Material Outgassing.....	19
6.4	Thermal Vacuum Bakeout.....	19
6.5	Hardware Handling.....	19
Chapter 7.0	Risk Management Requirements.....	20
7.1	General.....	20
7.2	Risk Management Plan.....	20
7.3	Risk List.....	21
Chapter 8.0	Integrated Independent Review Requirements.....	22
8.1	General Requirements.....	22
8.2	LDCM System Review Requirements.....	22
8.3	Component/Subsystem Review Requirements.....	22
Chapter 9.0	Design Verification Requirements.....	23
9.1	General Requirements.....	23
9.2	System Performance Verification Plan.....	23
9.3	System Performance Verification Matrix.....	23
9.4	Performance Verification Procedures.....	24
9.5	Environmental Verification Plan.....	24
9.6	Environmental Verification Specification.....	24
9.7	Environmental Test Matrix.....	24
9.8	Electrical Functional Test Requirements.....	25
9.8.1	Electrical Interface Tests.....	25
9.8.2	Aliveness Tests.....	25
9.8.3	Comprehensive Performance Tests (CPTs).....	25
9.8.4	Limited Performance Tests (LPTs).....	25
9.8.5	End-to-End Performance Tests.....	25
9.8.6	Failure-free Performance.....	26
9.9	Structural, Mechanical, and thermal Requirements.....	26
9.10	Electromagnetic Compatibility (EMC) Requirements.....	26
Chapter 10.0	Workmanship Standards.....	27
10.1	General Requirements.....	27

10.2	Applicable Documents/workmanship standards.....	27
10.3	Printed Wiring Boards (PWB).....	28
10.4	Ground Support Equipment (GSE).....	28
10.5	New/Advanced Packaging Technologies.....	28
10.6	Electrostatic Discharge Control.....	28
	10.6.1 Personnel Certification.....	29
	10.6.2 Protected Work Areas.....	29
	10.6.3 Packaging, Handling and Storage.....	29
Chapter 11.0	Parts Requirements.....	30
11.1	General.....	30
11.2	Developer’s Project Parts Engineer.....	30
11.3	Parts Control Board (PCB).....	31
	11.3.1 PCB Responsibilities.....	31
	11.3.2 PCB Meetings and Notification.....	31
	11.3.3 PCB Membership.....	31
11.4	Part Selection and Processing.....	32
	11.4.1 General.....	32
	11.4.2 Parts Selection.....	32
	11.4.3 Radiation Requirements for Part Selection.....	32
	11.4.4 Custom or Advanced Technology Devices.....	33
	11.4.5 Plastic Encapsulated Microcircuits (PEMs).....	34
	11.4.6 Verification Testing.....	34
	11.4.7 Parts Approved on Prior Projects.....	34
	11.4.8 Parts Used in Off-the-Shelf Assemblies.....	34
11.5	Part Analysis.....	35
	11.5.1 Destructive Physical Analysis.....	35
	11.5.2 Failed EEE Parts.....	35
	11.5.3 Failure Analysis.....	35
11.6	Additional Requirements.....	36
	11.6.1 Parts Age Control.....	36
	11.6.2 Derating.....	36
	11.6.3 GIDEP Alerts.....	36
	11.6.4 Prohibited Metals.....	36
	11.6.5 Traceability.....	36
	11.6.6 ESD Control.....	37
11.7	Parts Lists.....	37
	11.7.1 Parts Identification List (PIL).....	37
	11.7.2 Project Approved Parts List (PAPL).....	37
	11.7.3 As-Designed Parts List (ADPL).....	37
	11.7.4 As-Built Parts List (ABPL).....	37
11.8	Data Requirements.....	38
	11.8.1 General.....	38
	11.8.2 Retention of Data, Part Test Samples and Removed Parts.....	38
Chapter 12.0	Materials, and Processes Requirements.....	39
12.1	General Requirements.....	39
12.2	Materials and Processes Control Plan.....	39

12.3	Materials Selection Requirements	39
12.3.1	Fasteners.....	39
12.3.2	Flammability and Toxicity.....	40
12.3.3	Vacuum Outgassing.....	40
12.3.4	Shelf-Life-Controlled Materials	40
12.4	As-Designed/As-Built Materials and Processes List (M&P List)	40
12.4.1	Polymeric Materials.....	40
12.4.2	Inorganic Materials.....	40
12.4.3	Lubrication	40
12.4.4	Process Utilization list	41
Chapter 13.0	Ground Data Systems Assurance Requirements.....	47
13.1	General	47
13.2	Quality Management System.....	47
13.3	Requirements	47
13.4	Reviews	47
13.5	Assurance Activities.....	48
13.5.1	Concept Phase	48
13.5.2	Requirements Phase.....	48
13.5.3	Design Phase	49
13.5.4	Implementation Phase.....	50
13.5.5	Testing Phase.....	51
13.5.6	Operations and Maintenance Phase.....	53
13.5.7	Activities Performed throughout the Lifecycle.....	54
13.6	GFE, COTS, Existing and Purchased Software.....	55
13.6.1	COTS Management	55
13.7	Reuse Requirements.....	56
13.8	Defect Prevention Requirements.....	56
13.9	Databases	56
13.10	Security Assurance.....	57
13.11	Electromagnetic Compatibility Control	57
13.12	Reliability and Availability.....	57
13.12.1	Reliability Acceptance Testing.....	58
13.13	Maintainability Requirements.....	59
13.14	System Safety.....	60
Chapter 14.0	Applicable Documents List	61
Chapter 15.0	Acronyms.....	63
Chapter 16.0	Glossary	66

Chapter 1.0 Overall Requirements

1.1 GENERAL

This document, referred to as the “MAR,” defines Safety and Mission Assurance (SMA) requirements for the LDCM spacecraft/observatory development.

References to the “developer” or “contractor” in this document are directed to the spacecraft/observatory contractor. References to the “SAM” refer to the NASA GSFC LDCM Systems Assurance Manager (SAM). References to the “Government” or the “Project Office” refer to the NASA GSFC LDCM Project Office.

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

1. All flight hardware, that is designed, built, and/or provided by the developer or furnished by GSFC, from project initiation through launch and mission operations,
2. The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items,
3. All software critical for mission success.
4. The Ground Data System.

The developer shall ensure that managers of assurance activities 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. The developer’s Quality Manager shall interface with the NASA LDCM SAM on Safety and Mission Assurance activities. In the event that an SMA issue requires project management attention, the developer shall direct the issue to the Contracting Officer’s Technical Representative (COTR).

The requirements stated in this document apply to all work accomplished by the spacecraft/observatory developer and their suppliers of deliverable space flight hardware and software as applicable for the scope of the work to be accomplished. The developer shall ensure flow-down of and compliance to this MAR and system technical requirements to their suppliers as applicable.

1.2 SURVEILLANCE OF THE DEVELOPER

The work activities, operations, and documentation performed by the developer and/or his suppliers are subject to evaluation and inspection by government-designated representatives from GSFC, the Defense Contract Management Agency, or an independent assurance contractor. The LDCM project may delegate in-plant responsibilities and authority to these organizations via a letter of delegation, letter of assignment or task assignment.

The developer shall grant access to hardware, software and manufacturing and test facilities as well as supporting documentation to NASA representatives as necessary to support the government surveillance activities. The developer, upon request, shall provide government assurance representatives with documents, records, databases and equipment required to perform

their delegated duties. The developer shall provide the government assurance representative(s) with a work area within developer facilities appropriate for the activity to be performed.

1.3 APPLICABLE DOCUMENTS

To the extent referenced herein, applicable portions of the documents listed in Chapter 14 form a part of this document. The latest version of each document, at the time of the issue of the spacecraft/observatory Request for Offer (RFO), is applicable unless otherwise specified. In the event of a conflict between the documents listed in Chapter 14 and this requirements specification, the contents of this specification shall be considered the superseding requirements. In the event of a conflict between this Mission Assurance Requirements document and the Spacecraft Statement of Work (SOW), the SOW shall take precedence. In the event of any other unresolved conflict, the contracting officer shall be notified, and the order of precedence will be as directed by the contracting officer.

1.4 ACRONYMS AND GLOSSARY

Acronyms can be found in Chapter 15 Acronyms.

The definitions of words and terminology can be found in Chapter 16 Glossary.

DRAFT

Chapter 2.0 Quality Management System

2.1 GENERAL

The developer shall be compliant to the American National Standards Institute (ANSI)/ISO/American Society for Quality (ASQ) Q9001-2000. The developer shall supplement their Q9001 Quality Manual with a LDCM specific Systems Assurance Plan (CDRL SA-1) that defines on a chapter-by-chapter/section-by-section basis (referenced to the chapters of this document) how the developer will meet each requirement of this document. Every “shall” statement in this document is a requirement.

2.2 SUPPLEMENTAL QUALITY MANAGEMENT SYSTEM REQUIREMENTS

2.2.1 Control of Nonconforming Product

The developer shall implement a closed loop system for identifying and reporting nonconformances, ensuring that corrective action is implemented to preclude recurrence and verification of the adequacy of implemented corrective action by audit and test as appropriate. The system shall include a nonconformance review process, which shall consist of a Material Review Board (MRB).

2.2.2 Material Review Board

The developer shall implement a Material Review Board (MRB) to process the nonconformance 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 the project;
- e) Used as is upon concurrence with the project;
- f) MRB disposition actions shall also include request for a major waiver.

The MRB shall consist of a core team, including a NASA/Government representative, supplemented with other disciplines brought in as necessary. A developer representative responsible for ensuring that MRB actions are performed and implemented per developer procedures shall chair it. 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. The Contractor shall notify the NASA/Government representative prior to disposition of all MRB actions relating to flight hardware or ground support equipment (GSE) that interfaces with flight hardware.

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. The MRB close-out shall include documented objective evidence of the verification of effective corrective action.

2.2.3 Reporting of Failures

The developer shall report instances of failure to the GSFC Project Office within 24 hours of occurrence. Written Problem/Failure documentation shall be provided within 3 days of the initial notification (electronic notification is acceptable) (CDRL SA-2). The developer shall describe their processes for review, disposition, and approval of failure reports in applicable procedure(s) included, or referenced in the LDCM Systems Assurance Plan.

The developer shall report failures beginning with the first power application at the start of end item acceptance testing of the major component or subsystem, or the first operation of a mechanical item. Software Problem reporting shall begin with first use of the flight build software. The developer shall continue reporting failures through formal acceptance by the GSFC project office. The developer may use their own form upon request and approval by the GSFC project office. All discrepancies including root cause determination, corrective action, verification, and close out shall be documented and available for review by NASA throughout the implementation phase.

2.2.4 Control of Monitoring and Measuring Devices

The developer shall ensure that Testing and Calibration Laboratories used for LDCM fabrication, test and inspection hardware are compliant with the requirements of ISO 17025 – General Requirements for the Competence of Testing and Calibration Laboratories.

2.2.5 Flow-Down of Requirements

The developer shall flow down all LDCM MAR requirements to its suppliers as appropriate for the supplier's hardware and/or software. The developer shall ensure that its suppliers fulfill these requirements through the developer's contract review and purchasing processes, and the developer's procedures for documenting, communicating, and reviewing requirements with sub-tier suppliers.

2.2.6 Configuration Management

The developer shall perform configuration management (CM) in support of the LDCM Project in accordance with SOW paragraph 1.9.

2.3 GIDEP ALERTS AND PROBLEM ADVISORIES

The developer shall participate in the GIDEP (Government-Industry Data Exchange Program) in accordance with the requirements of the GIDEP Operations Manual (SO300- BT-PRO-010) and the GIDEP Requirements Guide (S0300-BU-GYD-010), available from the GIDEP Operations Center, Post Office (PO) Box 8000, Corona, California 92878-8000. For information on GIDEP, refer to the following web site: <http://www.gidep.org>.

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 GIDEP ALERTs, GIDEP SAFE-ALERTs, GIDEP Problem Advisories, GIDEP Agency Action Notices and NASA 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 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 S0300-BU-GYD-010 whenever failed or nonconforming items, available to other buyers, are discovered during the course of the contract.

DRAFT

Chapter 3.0 System Safety Requirements

3.1 GENERAL REQUIREMENTS

The developer shall implement a system safety program for the duration of the mission. The system safety program shall accomplish the following:

1. 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, ground support equipment, operations, and support facilities.
2. Meets the system safety requirements of the applicable range.
3. Meets the baseline industrial safety requirements of the institution where activity is performed.

3.2 DESIGN REQUIREMENTS

Specific safety requirements for design include the following:

- a. 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.
- b. 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, systems, or flight hardware.
- c. 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.

3.3 SYSTEM SAFETY PROGRAM PLAN (SSPP)

The developer shall prepare a System Safety Program Plan (SSPP) (CDRL SA-3) that describes the system safety implementation process which includes analysis and reduction or elimination of hazards that may cause the following:

- a. Loss of life or injury/illness to personnel
- b. Damage to or loss of equipment or property
- c. Unexpected or collateral damage as a result of tests

The SSPP shall specify the hazard analyses required to be performed on flight hardware, GSE, software and integration & test and prelaunch operations. These shall include a Preliminary Hazard Analysis (PHA) and Operations Hazard Analysis (OHA).

3.3.1 Preliminary Hazard Analysis

The developer shall perform and document a Preliminary Hazard Analysis (PHA) (CDRL SA-4) to identify safety critical areas, to provide an initial assessment of hazards, and to identify recommended hazard controls and follow-on actions. The developer shall perform and document a PHA 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 an acceptable level shall be included.

3.3.2 Operations Hazard Analysis

The developer shall perform an Operations Hazard Analysis (OHA) (CDRL SA-5) to examine procedurally controlled activities at the launch site or processing facilities. The OHA 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.

3.3.2.1 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 5.3 describes desired software safety activities to meet NASA HQ guidelines.

3.4 SAFETY REQUIREMENTS COMPLIANCE CHECKLIST

The developer shall demonstrate that the payload is in compliance with all safety requirements and any non-compliant areas have been identified. The developer shall document this in a Compliance Checklist (CDRL SA-6).

3.5 MISSILE SYSTEM PRELAUNCH SAFETY PACKAGE

The developer shall submit a Missile System Prelaunch Safety Package (MSPSP) (CDRL SA-7), consistent with the design maturity of the program. The content of each package shall be

consistent with the requirements of AFSPCMAN 91-710. Early in the design phase and continuing through the development effort, the ground operations hazards associated with the flight system, ground support equipment, and their interfaces shall be identified. The MSPSP shall include, as a minimum, a detailed description of the payload design sufficient to support hazard analysis results, hazard analysis method, and other applicable safety related information. All hazards affecting personnel, launch vehicle hardware, or the spacecraft shall be identified; instrument hazards addressed in their Safety Assessment Reports (CDRL SA-8) shall also be addressed. Hazard Reports are required as part of the MSPSP. In addition to identifying hazards, the MSPSP shall also identify the hazard controls, verifications, and tracking methods for each hazard, and establish a “closed loop” process to track each identified hazard.

A list of all hazardous/toxic materials and associated material safety data sheets shall be prepared and included in the final MSPSP.

3.5.1 Verification Tracking Log (VTL)

The developer shall establish a “closed loop” process for tracking all hazards to acceptable closure through the use of a Verification Tracking Log (VTL) (CDRL SA-9). Any hazard controls still open at Phase 3 shall be listed in the VTL and tracked to closure. 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 first operational use/restraint.

3.5.2 Ground Operations Procedures

The developer shall submit all ground operations procedures to be used at the launch site to the LDCM Project for review before submittal to the launch range (CDRL SA-10). Launch site ground operations procedures shall be submitted to Range Safety 45 days prior to use. The LDCM Project reserves the right to review, upon request, contractor site operations procedures to ensure compliance.

3.5.3 Safety Variance

When a specific safety requirement cannot be met, the developer shall submit an associated safety variance, per NPR 8715.3 which identifies the hazard and shows the rationale for approval of a variance (CDRL SA-11). 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.
- 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 shall be accompanied by documentation as to why the requirement can not be met, the risks 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 personnel safety).

3.6 SUPPORT FOR SAFETY WORKING GROUP MEETINGS

The developer shall provide technical support 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 the project or range personnel to discuss any situations that may arise with respect to overall project safety.

3.7 MISHAP REPORTING AND INVESTIGATION

The developer shall report any mishaps, incidents, hazards, and close calls via an Accident/Incident Mishap Report to the LDCM Project Manager.

3.8 ORBITAL DEBRIS ASSESSMENT

The developer shall prepare an Orbital Debris Assessment consistent with NPD 8710.3B, Policy for Limiting Orbital Debris Generation and NSS 1740.14, Guidelines and Assessment Procedures for Limiting Orbital Debris (CDRL SA-12).

Chapter 4.0 Reliability and Probabilistic Risk Assessment

4.1 GENERAL REQUIREMENTS

The developer shall implement a reliability program applicable to the development of all software and hardware products and processes. The developer shall provide a Reliability Program Plan describing the planned approach and schedule for the project reliability activities, including performance of a Probabilistic Risk Assessment (PRA), with the proposal. The developer shall identify in the plan the reliability tasks to be performed and how those tasks will be implemented and controlled. The developer shall discuss the scheduling of the reliability tasks relative to project milestones. The developer shall ensure reliability functions are an integral part of the design and development process and the reliability functions interact effectively with other project disciplines, including systems engineering, hardware design, and product assurance. The developer shall describe how reliability assessments are integrated with the design process and other assurance practices. The developer shall describe how failure definitions and alternate and degraded modes of operations that include credible failure conditions could be mitigated by implementing workarounds. The developer shall describe the integration of reliability activities with the probabilistic risk assessment process.

4.2 PROBABILISTIC RISK ASSESSMENT

The developer shall provide a Limited Scope Probabilistic Risk Assessment (PRA) (CDRL SA-13) commensurate with a Class B mission as defined NPR 8705.4, Risk Classification for NASA Payloads, and in accordance with the requirements of NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects. A limited scope PRA is of the same general rigor as a full-scope PRA, but focuses on the mission-related end-states of specific decision-making interest, instead of all applicable end states.

Potential candidates for PRA analyses may come from mission operational working group meetings, reliability working group (RWG) meetings, safety hazard analyses, instrument and observatory FMEA, Instrument and Spacecraft Reliability Prediction Analyses, I&T Problem reports, etc. The observatory developer shall identify and use the appropriate types of analyses for each scenario modeled, and the modeling tools and techniques to be used (e.g., Master Logic Diagrams (MLD), Failure Mode and Effects Analysis (FMEA), Fault Tree Analyses (FTA), Event Tree Analyses (ETA), and/or Event Sequence Diagrams).

The developer shall use the PRA to quantify risk and uncertainties associated with identifying pivotal events or scenarios that may cause a mission-ending failure or human safety hazardous condition. The developer shall implement the PRA procedures across every phase of the project life cycle while improving and updating the PRA with current information.

The developer shall submit the PRA to the project office for approval, and shall present results of the PRA at all design reviews, beginning with the Preliminary Design Review (PDR)

Presentations shall include design trade-study results and PRA results impacting design or risk decisions.

4.3 RELIABILITY ANALYSES

The developer shall ensure that reliability analyses are performed during the design phase so that identified problem areas can be addressed and any required corrective action can be taken in a timely manner.

4.3.1 Failure Modes and Effects Analysis and Critical Items List

The developer shall perform a Failure Modes and Effects Criticality Analysis (FMECA) early in the design phase to identify potential failure modes during each phase of the mission, and the effect of those failures on related systems and the mission. As changes to the design are made, the developer shall revise the FMECA to reflect the current design. Failure modes shall, at a minimum, be assessed at the circuit card level, assessing each potential failure mode for the effect at the level of analysis (circuit level), the next higher level, and the mission level. The FMECA shall be performed in accordance with guidance provided in the Data Item Description. The developer shall use the results of the FMECA to evaluate the design against requirements. The developer shall ensure identified discrepancies are evaluated by management and design groups to determine the need for corrective action.

A Critical Items List (CIL) shall be developed from those failure modes that could result in serious injury, loss of life or loss of launch vehicle whether the result of single point failures or redundant failures, and shall include single point failures that could result in loss of one or more mission objectives. For each critical item, retention rationale shall be provided that describes justification for retaining the potential failure in the design. Retention rationale shall consist of design features, test, inspection, heritage and flight history, operational considerations, workarounds, etc., that reduce the likelihood of the failure occurring and reduce the potential consequences if the failure occurs.

The developer shall submit the FMECA (CDRL SA-14) and CIL (CDRL SA-15) to the project office, and shall present results of the FMECA and CIL at all design reviews, beginning with the Preliminary Design Review (PDR). Presentations shall include design trade-study results and FMECA results impacting design or risk decisions.

4.3.2 Fault Tree Analysis

The developer shall prepare Fault Tree Analyses (FTAs) (CDRL SA-16) that address both mission failures and degraded modes of operation. FTA Analyses shall be performed and integrated as part of the PRA process. 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 that undesired state. Component hardware/software failures, external hardware/software failures, and human factors shall be considered in the analysis.

The developer shall present results of the FTA at all design reviews, beginning with the Preliminary Design Review (PDR). Presentations shall include design trade-study results and FTA results impacting design or risk decisions.

4.3.3 Parts Stress Analyses

The developer shall perform stress analyses on Electrical, Electronic, and Electromechanical (EEE) parts and devices, as applied in circuits within each component for conformance with EEE-INST-002. The analyses shall be performed at the most stressful part-level parameter values that can result from the specified performance and environmental requirements on the assembly or component. The analyses shall be performed in close coordination with the packaging reviews and shall be required input data for component-level design reviews. The analyses shall be documented and maintained current to the latest design. The developer shall provide the analyses, summary sheets, and revisions (CDRL SA-23) to the Project Office. Analyses results shall be presented at all design reviews beginning with PDR. Presentations shall include design trade-study results and Parts Stress Analyses results impacting design or risk decisions.

4.3.4 Worst-Case Analyses

The developer shall perform worst-case analyses for mission or science-critical parameters that are subject to variations that could degrade performance, where failure results in a severity category of 2 or higher, and provides data that question the flightworthiness of the design. Analyses or test or both shall demonstrate adequacy of margins in the design of electronic circuits, optics, electromechanical and mechanical items (mechanisms). The analyses shall consider all parameters set at worst-case limits due to manufacturing variability and worst-case environmental (including radiation) and aging stresses for the parameter or operation being evaluated. The analyses shall be updated in keeping with design changes. The developer shall provide the analyses, summary sheets, and revisions (CDRL SA-24) to the Project Office. The analyses and updates shall be presented at all design reviews beginning with PDR. Presentations shall include design trade-study results and Worst Case Analysis results impacting design or risk decisions.

4.3.5 Numerical Assessments and Predictions

The developer shall perform comparative numerical assessments and/or reliability predictions to:

1. Assist in trade-studies by evaluating alternative design concepts, redundancy and cross strapping approaches, and part substitutions;
2. identify the elements of the design which are potentially the greatest detractors of system reliability;
3. identify those potential mission limiting elements and components that will require special attention in part selection, testing, environmental isolation, and/or special operations;
4. evaluate the design in terms of mission success requirements
5. evaluate the impact of proposed engineering changes and waiver requests on reliability.

The developer shall describe in their assessments the level of detail of a model suitable for performing the intended functions enumerated above. The results of the reliability assessments shall be reported at design reviews starting with PDR. The presentations shall include comments on how the analyses were used to perform design trade-offs or how the results were taken into consideration when making design or risk management decisions.

4.4 LIMITED-LIFE ITEMS

The developer shall provide a plan to identify and manage limited life items. The developer shall submit the Limited-Life Items Plan (CDRL SA-25). In the plan, the developer shall define limited-life items, the impact on mission parameters, responsibilities for mitigating limited-life items, and provide a list of limited-life items, including data elements as follows:

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

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

The developer shall list limited-life items including selected structures, thermal control surfaces, solar arrays and electromechanical mechanisms. The developer shall consider atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue to identify limited-life thermal control surfaces and structure items; the developer shall include mechanisms such as batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, gyros, actuators and scan devices when aging, wear, fatigue and lubricant degradation limit their life.

The developer shall maintain records allowing for evaluation of cumulative stress (time and cycles) for limited-life items, starting when useful life is initiated, and indicating the project activity that stresses the items.

The developer shall obtain a program waiver approval by GSFC when the use of an item whose expected life is less than its mission design life.

4.5 CONTROL OF SUB-DEVELOPERS AND SUPPLIERS

The developer shall ensure that system elements obtained from sub-developers and suppliers meet project reliability requirements. All subcontracts shall include provisions for review and evaluation of the sub-developers' and suppliers' reliability efforts by the prime developer at the prime developer's discretion, and by GSFC at its discretion. The developer shall tailor the reliability requirements of this document in hardware and software subcontracts for the project. The developer shall exercise necessary surveillance to ensure that sub-developer and supplier reliability efforts meet overall system requirements.

The developer shall ensure the tailored requirements:

- Incorporate quantitative reliability requirements in subcontracted equipment specifications.
- Assure that sub-developers have reliability programs that are compatible with the overall program
- Review sub-developer assessments and analyses for accuracy and correctness of approach.
- Review sub-developer test plans, procedures and reports for correctness of approach and test details.
- Attend and participate in sub-developer design reviews.
- Ensure that sub-developers, during the project operational phase, comply with the applicable system reliability requirements.

4.6 RELIABILITY 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 developer shall use the reliability data provided by the Project Office to perform the reliability analyses. The developer shall formally notify the Project Office promptly when examination of the data or testing by the developer indicates that the reliability or maintainability of Government Furnished Equipment is inconsistent with the reliability requirements of the overall system

4.7 SUPPORT FOR RELIABILITY WORKING GROUP MEETINGS

The developer shall provide technical support to the Project for Reliability Working Group (RWG) meetings, and technical reviews, as required.

The RWG will meet as necessary, and as convened by the project personnel, to review reliability requirements and analyses, to assist in resolving reliability issues and concerns, and to discuss any situations that may arise with respect to overall mission reliability.

4.8 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.

4.8.1 Trend Analyses

Parameter trend analyses is a companion approach to analytical reliability models. In general, known values of certain parameters can directly impact on a component or systems reliability, even though the exact quantitative relationship may not have been determined. Those measurable parameters that directly affect system or component reliability, when sampled over time can be examined to determine if there is a pattern of deviation over time (i.e., a trend) from acceptable performance limits. In this manner, it may be possible to predict future parameter values, or at least estimate the long-term range of values of these influential variables. Thus, if these

parameters are trending towards hazardous or unacceptable levels, the potential problem could be identified prior to the occurrence of high-risk situations.

The developer shall assess subsystems and components to determine measurable parameters that relate to performance stability and reliability. The developer shall perform trending in accordance with the SOW paragraph 2.5.

4.8.2 Analysis of Test Results

The developer shall analyze test information, trend data and failure investigations to evaluate reliability implications. The developer shall document identified problem areas, and ensure developer management takes corrective action. The developer shall include this information in progress reports to the Project, or in a separate monthly report. The developer shall report results of analyses at design reviews. The developer shall address in the report design trade studies and reliability prediction results impacting design or risk decisions.

4.9 SOFTWARE RELIABILITY

Refer to Section 5.4 for software reliability requirements.

Chapter 5.0 Software Assurance Requirements

5.1 SOFTWARE ASSURANCE

The developer's Software Assurance program shall address software assurance disciplines (i.e., Software Quality, Software Safety, Software Reliability, Verification and Validation, and Independent Verification and Validation) 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 document in The LDCM Systems Assurance Plan (CDRL SA-1) how the Software Assurance Requirements will be met.

5.2 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.

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.

5.3 SOFTWARE SAFETY

The developer shall ensure that safety considerations are 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 ensure that their approach to the software safety program is documented in the System Safety Program Plan as appropriate.

The developer shall ensure that software safety requirements are clearly identified, documented, tracked, and controlled throughout the lifecycle. The developer shall identify potential hazards and ensure implementation of safety critical requirements. 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 document in operational documentation all safety-related commands, data, input sequences and workarounds necessary for the safe operation of the system. The developer shall report on all software safety requirements, software safety issues and risks at all formal system-level reviews.

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.

5.4 SOFTWARE RELIABILITY

The developer shall ensure that software reliability is incorporated into their software products. The developer shall ensure that appropriate activities are planned to support the achievement and verification of the developer's software reliability requirements.

5.5 VERIFICATION AND VALIDATION

- a. The developer shall plan and implement a Verification and Validation (V&V) program in accordance with the SOW Paragraph 4.4.

5.6 INDEPENDENT VERIFICATION AND VALIDATION

The developer shall support NASA IV&V activities in accordance with the SOW paragraph 4.4.

5.7 GFE, EXISTING AND PURCHASED SOFTWARE

If the developer is provided software as government-furnished equipment (GFE), or will use existing or purchased software and firmware, the developer shall verify that the software and firmware meets the functional, performance, and interface requirements placed upon it. The developer shall ensure that the software and firmware meets applicable standards, including those for design, code, and documentation, or shall secure a LDCM Project waiver to those standards. Any significant modification to any piece of the existing software shall be subject to the provisions of the developer's quality management system and the provisions of this document. A significant modification is defined as the change of twenty percent of the lines of code in the software.

Chapter 6.0 Contamination Control

6.1 GENERAL REQUIREMENTS

The developer shall plan and implement a contamination control program for LDCM hardware. The developer shall establish specific cleanliness requirements and the approach to meet the requirements in a Contamination Control Plan (CCP) (CDRL SA-17).

6.2 CONTAMINATION CONTROL PLAN

The developer's CCP shall describe the procedures that shall be followed to control contamination. The CCP shall define a contamination allowance for performance degradation of contamination sensitive hardware such that, even in the degraded state, the hardware will meet its mission objectives. The CCP 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 integration, test, pre-launch and launch activities.

6.3 MATERIAL OUTGASSING

The developer shall determine material vacuum outgassing in accordance with ASTM E-595. Individual material outgassing data shall be established based on each component's operating conditions. Established material outgassing data shall be verified and shall be provided to the GSFC LDCM Project for review and approval upon request.

6.4 THERMAL VACUUM BAKEOUT

The developer shall perform thermal vacuum bakeouts of hardware as required to protect contamination-sensitive components. The parameters of such bakeouts (e.g., temperature, duration, outgassing requirements, and pressure) shall be individualized depending on materials used, the fabrication environment, and the established contamination allowance. Thermal vacuum bakeout results shall be verified and shall be provided to the GSFC LDCM Project for review and approval upon request.

A quartz crystal microbalance (QCM), or temperature controlled quartz crystal microbalance (TQCM), and cold finger shall be incorporated during all thermal vacuum bakeouts at the box, instrument and spacecraft level. These devices shall provide additional information to enable a determination of the duration and effectiveness of the thermal vacuum bakeout as well as compliance with the CCP.

6.5 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.

Chapter 7.0 Risk Management Requirements

7.1 GENERAL

The developer shall implement an organized, systematic decision-making process for Continuous Risk Management (CRM) process to increase the likelihood of achieving program/project goals. The CRM process shall apply to all aspects of the program/project. This process shall identify, analyze, plan (for the handling of risks), track, control, communicate and document all project risks. The developer shall:

- a. Search for, identify, and document all project risks (before they become problems);
- b. Evaluate, classify, and prioritize all identified risks;
- c. Plan and implement risk mitigation strategies, actions, and tasks (and assign appropriate resources);
- d. Track risks being mitigated, collect data to capture risk attributes and mitigation information, establish performance metrics, examine trends, and analyze deviations and anomalies;
- e. Control risks by closeout, re-planning, contingency planning, or continued tracking and execution of the current plan;
- f. Document risk information and communicate to all levels of the project;
- g. Report on outstanding risk items at all management and design reviews.

The developer shall implement a systems management approach that formalizes and integrates the CRM process throughout the system life cycle. All elements of the system shall be addressed (e.g., flight, ground and launch vehicle segments, hardware and software, critical ground support equipment). All phases of the life cycle shall be considered (e.g., fabrication, assembly, integration and test, environmental testing, transportation, launch site processing, launch deployment, in-orbit check out, operations decommissioning).

7.2 RISK MANAGEMENT PLAN

The developer shall document the project-specific implementation of the CRM process in a Risk Management Plan (RMP) (CDRL PM-10). 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 tools and techniques that will be used to manage the risks. The NPR 7120.5, "NASA Program and Project Management Processes and Requirements," is the controlling requirements used in the preparation of this plan.

The developer shall document and report all identified risks in accordance with the developer's RMP. Identified risk areas shall be addressed at project status reviews and at Integrated Independent Reviews. The developer shall ensure that risks are addressed with mitigation and acceptance strategies.

7.3 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.

For each primary risk (those having both high probability and high impact/severity), the developer shall prepare and maintain the following:

- a. Description of the risk, including primary causes and contributors, actions embedded in the program or project to date to reduce or control it, and information collected for tracking purposes.
- b. Primary consequences should the undesired event occur.
- c. 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.
- d. 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.
- e. Characterization of a primary risk as “acceptable” shall be supported by a rationale (with the concurrence of the Governing PMC) that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

Chapter 8.0 Integrated Independent Review Requirements

8.1 GENERAL REQUIREMENTS

The developer shall support a series of comprehensive system-level technical reviews that will be conducted by the GSFC Office of Systems Safety and Mission Assurance (OSSMA) Systems Review Office (SRO). These reviews cover all aspects of flight and ground hardware, software, and operations for which the developer has responsibility. In addition, each developer shall conduct a program of peer reviews at the component and subsystem level.

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

- a. Develop and organize material for oral presentation to the GSFC LDCM review team. Copies of the presentation material shall be available at each review.
- b. Support splinter review meetings resulting from the major review.
- c. Produce written responses to recommendations and action items resulting from the review.
- d. Summarize, as appropriate, the results of the peer reviews at the component and subsystem level.

8.2 LDCM SYSTEM REVIEW REQUIREMENTS

The contractor shall meet the requirements of SOW paragraph 1.2 for reviews.

8.3 COMPONENT/SUBSYSTEM REVIEW REQUIREMENTS

The developer shall plan and implement a program of peer reviews at the component and subsystem levels. The developer shall ensure that peer reviews are conducted during all phases of the project life. The developer shall provide notification to the LDCM project of the peer reviews scheduled prior to holding the review.

The peer reviews should evaluate the ability of the component or subsystem to successfully perform its function 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, should be addressed at the peer reviews. Electrical interconnection harness design and assembly requirements should be addressed.

The packaging reviews should 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 and substrates and their interconnections in the component design.
- c. Provisions for protection of the parts and ease of inspection.

The developer shall ensure that peer reviews are conducted by personnel who are not directly responsible for design of the hardware under review.

Chapter 9.0 Design Verification Requirements

9.1 GENERAL REQUIREMENTS

The developer shall conduct a verification program to ensure that the system meets mission requirements. The program shall consist of functional demonstrations, analytical investigations, physical measurements and tests that simulate all expected environments.

The Verification Program begins with functional testing of assemblies. It continues through functional and environmental testing supported by appropriate analysis, at the component, subsystem/instrument and spacecraft/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, and the appropriate Ground Data System elements.

The General Environmental Verification Specification (GEVS) for GSFC Flight Programs and Projects (GSFC-STD-7000) shall be used as a baseline guide for developing the verification program. Alternative methods are acceptable provided that the net result demonstrates compliance with the intent of the requirements.

9.2 SYSTEM PERFORMANCE VERIFICATION PLAN

A System Performance Verification Plan (CDRL SE-9) shall be prepared and implemented (reference GEVS Section 2.1). The plan shall define the tasks and methods required to verify the ability of the system to meet each specified mission requirement (structural, thermal, optical, electrical, guidance/control, RF/telemetry, science, mission operational, etc.), including records documenting compliance. Limitations in the ability to verify any performance requirement shall be addressed, including the addition of supplemental tests and/or analyses that will be performed and a risk assessment of the inability to fully 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.

9.3 SYSTEM PERFORMANCE VERIFICATION MATRIX

The developer shall maintain documentation to demonstrate compliance with each system performance requirement. The developer shall maintain a matrix (CDRL SE-22), or equivalent system, that shows the flow-down of each performance requirement and the verification process. The matrix shall be iterated as verification is completed, kept current, and the status made available upon request. The matrix shall be included in the system review data packages showing the current verification status.

9.4 PERFORMANCE VERIFICATION PROCEDURES

For each performance verification test activity conducted at the subsystem, spacecraft and observatory levels (or other appropriate levels) of assembly, the developer shall prepare procedures for verifying compliance with each system performance requirement. These procedures shall identify the verification article configuration and provide detailed instructions for accomplishing and documenting the verification activity. As-run copies of these procedures shall be available for reference at the developer's facility.

Verification 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 shall also address safety and contamination control provisions as appropriate.

9.5 ENVIRONMENTAL VERIFICATION PLAN

The developer shall prepare an Environmental Verification Plan (EVP) as part of the system performance verification plan to prescribe the tests and analyses which will collectively demonstrate that the hardware and software comply with the environmental verification requirements. The EVP 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 requirement 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 activity shall be described.

Limitations in the environmental verification program that preclude 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 the project risk shall be included in the System Performance Verification Plan.

9.6 ENVIRONMENTAL VERIFICATION SPECIFICATION

As part of the System Performance Verification Plan, the developer shall prepare an environmental verification specification 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.

9.7 ENVIRONMENTAL TEST MATRIX

As an adjunct to the system Environmental Verification Plan, the developer shall maintain a matrix, or equivalent system, that identifies all environmental tests that will be performed on each component, subsystem, and spacecraft clearly showing each environmental exposure and test article level of assembly. The purpose is to provide a ready reference to the contents of the environmental 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 matrix. The matrix shall be iterated as performance is completed, kept current, and the status made available upon request. The matrix shall be

prepared in conjunction with the initial environmental verification plan and shall be updated as the project matures. This matrix may be combined with the Performance Verification Matrix. The matrix shall be included in the system review data packages showing the current status.

9.8 ELECTRICAL FUNCTIONAL TEST REQUIREMENTS

9.8.1 Electrical Interface Tests

As a part of the integration of a component or subsystem into the next higher level of assembly, the developer shall perform electrical tests (reference GEVS Section 2.3.1) to verify the interface configuration (power, grounds, commands, telemetry, signals, timing, etc.). Prior to mating with other hardware, electrical harnessing shall be tested to verify the wire routing, isolation, impedance, and overall workmanship. The following parameters shall be verified as a minimum:

- a. Accuracy (signals on correct pins and nowhere else),
- b. Inputs and outputs (unloaded and loaded),
- c. Specified range (high/low extremes as well as nominal),
- d. Range impacts (how range extremes of one signal affect related signals).

9.8.2 Aliveness Tests

An aliveness test shall be performed as necessary to verify that the subsystem, payload, spacecraft and/or observatory and its major components are functioning.

9.8.3 Comprehensive Performance Tests (CPTs)

The developer shall perform CPTs at the subsystem, spacecraft, payload and observatory levels of assembly (reference GEVS Section 2.3.2). The CPT shall be a detailed demonstration that the hardware and software meet their performance requirements. The CPT shall demonstrate the operation of redundant circuitry and satisfactory performance in all operational modes. CPTs shall demonstrate that, with the application of known stimuli and appropriate inputs, the test article will produce the expected responses and outputs. The initial CPT shall serve as a baseline against which the results of all later CPTs shall be readily compared.

9.8.4 Limited Performance Tests (LPTs)

The developer shall conduct LPTs at the subsystem, spacecraft, payload and observatory levels of assembly when CPTs are not warranted to demonstrate that the functional capability has not been degraded (reference GEVS Section 2.3.3). The LPT shall be a demonstration that the hardware and software meet their performance requirements. The LPT shall demonstrate the operation of redundant circuitry and satisfactory performance in selected operational modes. LPTs shall demonstrate that, with the application of known stimuli and appropriate inputs, the test article will produce the expected responses and outputs within acceptable limits. The initial LPT shall serve as a baseline against which the results of all later LPTs can be readily compared.

9.8.5 End-to-End Performance Tests

Prior to the Observatory Pre-Ship Review, the developer shall perform an end-to-end compatibility test to demonstrate the ground system capability to communicate with the Observatory (up-link and down-link) via the ground to space network (reference GEVS Section 2.8). Simulated normal orbital mission scenarios encompassing launch, systems turn-on, housekeeping, command/control, and stabilization/pointing shall be demonstrated, including the

collecting, processing, and archiving of science data. The Observatory immunity to erroneous commands, autonomous safe-hold, and simulated anomaly recovery operations shall also be demonstrated.

9.8.6 Failure-free Performance

At the conclusion of the performance verification program, the observatory shall have demonstrated minimum reliability by failure-free performance for at least the last 350 hours of testing prior to shipment to the launch site. Failure-free operation during the thermal vacuum test and during ambient testing of the integrated observatory may be included as part of the demonstration. Hardware changes prior to shipment to the launch site shall invalidate previous demonstration.

9.9 STRUCTURAL, MECHANICAL, AND THERMAL REQUIREMENTS

The developer shall demonstrate compliance with specified structural and mechanical requirements through a series of interdependent test and analysis activities. These demonstrations shall verify design and specified factors of safety to ensure spacecraft interface compatibility, acceptable workmanship, and material integrity.

When planning the tests and analyses, the developer shall consider all expected environments, including the following:

- Structural loads (reference GEVS Section 2.4.1)
- Mass properties (reference GEVS Section 2.4.7)
- Mechanical mechanism functions (reference GEVS Section 2.4.5)
- Vibration (acoustics, 3-axis sine sweep and random) (reference GEVS Sections 2.4.2, 2.4.3)
- Mechanical shock (self induced, externally induced) (reference GEVS Section 2.4.4)
- Thermal balance (reference GEVS Section 2.6.3)
- Thermal vacuum (reference GEVS Section 2.6)

9.10 ELECTROMAGNETIC COMPATIBILITY (EMC) REQUIREMENTS

The developer shall ensure that hardware is designed in accordance with the systems performance requirements (reference GEVS Section 2.5) so that:

- a. The observatory, its subsystems and components shall not generate electromagnetic interference that could adversely affect its own elements, including the instruments or the safety and operation of the launch vehicle and launch site.
- b. The observatory, its subsystems and components shall not be susceptible to emissions that could adversely affect their safety and performance. This applies whether the emissions are self-generated or derived from other sources or whether they are intentional or unintentional.

Chapter 10.0 Workmanship Standards

10.1 GENERAL REQUIREMENTS

The developer shall plan and implement an Electronic Packaging and Processes Program to assure that all electronic packaging technologies, processes, and workmanship activities selected and applied meet mission objectives for quality and reliability.

10.2 APPLICABLE DOCUMENTS/WORKMANSHIP STANDARDS

The developer shall use the NASA preferred standards identified in the NASA technical standards program in the NASA Online Directives Information System (NODIS). For access to these documents, use the following hyperlink: <http://standards.nasa.gov/>

- a. Conformal Coating and Staking: NASA-STD-8739.1, Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies;
- b. Soldering – Flight, Surface Mount Technology: NASA-STD-8739.2, Surface Mount Technology;
- c. Soldering – Flight/GSE to Flight Interface, Manual (hand): NASA-STD-8739.3, Soldered Electrical Connections;
- d. Soldering – Ground Systems: IPC/EIA J-STD-001C, Requirements for Soldered Electrical and Electronic Assemblies;
- e. Electronic Assemblies – Ground Systems: IPC-A-610C, Acceptability of Electronic Assemblies;
- f. Crimping, Wiring, and Harnessing: NASA-STD-8739.4, Crimping, Interconnecting Cables, Harnesses, and Wiring;
- g. Fiber Optics: NASA-STD-8739.5, Fiber Optic Terminations, Cable Assemblies, and Installation;
- h. Electrostatic Discharge Control (ESD): ANSI/ESD S20.20-1999 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)
- i. Printed Wiring Board (PWB) Design:
 - IPC 2221 Generic Standard on Printed Wiring Board Design and
 - IPC 2222, Sectional Design Standard for Rigid Organic Printed Boards;
 - IPC-2223, Sectional Design Standard for Flexible Printed Boards;
- j. Printed Wiring Board 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: IPC 6012B Qualification and Performance Specification for Rigid Printed Boards: all flight boards shall be compliant to the Performance Specification Sheet for Space and Military Avionics (SMA Specification Sheet) class 3/A product. In the event of a conflict between the Design and Manufacture Specifications, the SMA specification shall take precedence.

IPC-6013, Qualification and Performance Specification for Flexible Printed Boards.

The current status and/or any application notes for these standards can be obtained at URL <http://standards.nasa.gov>.

Alternate workmanship standards may be used when approved by the GSFC LDCM Project. The developer shall submit the alternate standard for GSFC LDCM Project approval prior to use.

10.3 PRINTED WIRING BOARDS (PWB)

The PWB manufacturing and acceptance requirements identified in this chapter are based on using PWBs designed in accordance with the PWB design standards referenced in Section 10.2. The developer shall ensure that space flight PWB designs do 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.).

The developer shall provide PWB test coupons (CDRL SA-18) to the GSFC Materials Engineering Branch (MEB) or a GSFC/MEB approved laboratory for evaluation. Results of evaluation shall be made available to the developer.

10.4 GROUND SUPPORT EQUIPMENT (GSE)

The developer shall ensure that GSE assemblies, that interface directly with space flight hardware, shall be designed and fabricated using space flight parts, materials, and processes for any portion of the assemblies (connectors, test cables, etc.) that mate with the flight hardware or will reside with the space flight hardware in environmental chambers or other test facilities that simulate a space flight environment.

10.5 NEW/ADVANCED PACKAGING TECHNOLOGIES

New and/or advanced packaging technologies (multi-chip modules (MCMs), stacked memories, chip on board, etc.) that have not previously been used in space flight applications shall be reviewed and approved through the Parts Control Board (PCB). The developer shall include new/advanced technologies as part of the Parts Lists.

10.6 ELECTROSTATIC DISCHARGE CONTROL

The developer shall document and implement an ESD Control Program, compliant with ANSI/ESD S20.20, Protection of Electrical and Electronic Parts, Assemblies and Equipment (excluding electrically initiated explosive devices). The program shall protect the most sensitive parts involved in the project and ensure that all manufacturing, inspection, testing, and other processes will not compromise mission objectives for quality and reliability due to ESD events.

At a minimum, the ESD Control Program shall address training, protected work area procedures and verification schedules, packaging, facility maintenance, handling, storage, and shipping.

10.6.1 Personnel Certification

The developer shall ensure that all personnel who manufacture, inspect, test, otherwise process electronic hardware, or require unescorted access into ESD protected areas are certified as having completed the required training, appropriate to their involvement prior to handling any electronic hardware.

10.6.2 Protected Work Areas

The developer shall ensure that electronic hardware is manufactured, inspected, tested, or otherwise processed only at designated ESD protective work areas. The developer shall verify these work areas shall be verified on a regular schedule as identified in the developer's ESD Control Program documentation.

10.6.3 Packaging, Handling and Storage

The developer shall ensure that electronic hardware is properly packaged in ESD protective packaging at all times when not actively being manufactured, inspected, tested, or otherwise processed. Materials selected for packaging or protecting ESD sensitive devices shall not leach chemicals, leave residues, or otherwise contaminate parts or assemblies. Any electronic parts needing very low ESD control should be identified to procurement receiving and incoming inspection personnel.

Chapter 11.0 Parts Requirements

11.1 GENERAL

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 part selection processes for the duration of the contract.

The developer shall prepare a Parts Control Plan (PCP) (CDRL SA-19) 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 plan shall address how the developer ensures the flow down of the applicable parts control requirements to the suppliers.

The developer shall select and process all parts in accordance with EEE-INST-002, GSFC EEE Parts Selection, Screening, Qualification and Derating, for part quality level 2 or better. Exceptions for use of a lesser grade part with additional testing shall only be made on a case by case basis when a level 2 part is not available. Such exceptions require approval by the Parts Control Board (PCB). The developer shall control the selection, application, evaluation, and acceptance of all parts through the PCB.

11.2 DEVELOPER'S PROJECT PARTS ENGINEER

The developer shall designate one key individual to be their Project Parts Engineer (PPE). The PPE shall have the prime responsibility for management of their EEE parts control program. This individual shall have direct, independent and unimpeded access to the GSFC PPEs and Parts Control Board. The PPE shall work with design engineers, radiation engineers, reliability engineers and the GSFC PPE to perform part selection and control.

Tasks performed by the developer PPE shall include but are not limited to the following:

1. Work with GSFC PPE team to perform parts control.
2. Provide PCB agenda, prepare Parts Lists and provide supporting part information for parts evaluation and approval by the PCB.
3. Coordinate Parts Control Board meetings, maintain minutes, develop and maintain the spacecraft's Parts Identification List (PIL), develop the spacecraft portion of the Project Approved Parts List (PAPL), As-Designed Parts List (ADPL) and As-Built Parts List (ABPL).
4. Perform Customer Source Inspections (CSI) and audits at supplier facilities as required.
5. Prepare part procurement, screening, qualification, and modification specifications, as required.

6. Disposition/track part nonconformances and part failure investigations.
7. Track and report impact of Alerts and Advisories on flight hardware.

11.3 PARTS CONTROL BOARD (PCB)

The developer shall establish a Parts Control Board (PCB) 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, and for developing and maintaining the PAPL for the spacecraft. In addition, the PCB is responsible for providing assistance for 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.

11.3.1 PCB Responsibilities

The PCB responsibility shall include but not limited to the following:

- Evaluation of EEE parts for conformance to established criteria and inclusion in the PAPL,
- Develop and maintain the PAPL PIL, ADPL and ABPLs for the spacecraft.
- 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.

If there are any parts issues that cannot be resolved at the PCB level, the issues shall be elevated as appropriate.

11.3.2 PCB Meetings and Notification

The developer shall convene PCB meetings as needed. The GSFC Project Parts Engineer will be a permanent voting member for PCB actions. The developer's PPE shall maintain meeting minutes or records to document all decisions made.

The developer PPE shall notify attendees at least five (5) working days in advance of upcoming meetings. Notification of PCB meetings shall include a proposed agenda and documentation necessary to conduct the review.

11.3.3 PCB Membership

As a minimum, the PCB membership shall consist of the developer's Product Assurance Manager, developer PPE, GSFC Project PPE and GSFC Project Radiation Engineer (PRE) when required. The participation of the developer PPE and GSFC PPE is required for all PCB meetings. 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.

11.4 PART SELECTION AND PROCESSING

11.4.1 General

All part commodities identified in EEE-INST-002 is considered EEE parts and shall be subject to the requirements set forth in this chapter. EEE Parts types that do not fall in to any of the categories covered in EEE-INST-002 shall be reviewed by the PCB and evaluated using the closest NASA, DSCC or government controlled specification. In the event a suitable government baseline specification does not exist, the PCB shall identify the best available industry standard for that particular commodity, and develop appropriate procurement, screening and qualification specification.

11.4.2 Parts Selection

The developer shall select parts according to the GSFC EEE Parts Selection, Screening, Qualification and Derating document (EEE-INST-002) 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, and such exceptions require approval by the PCB. The use of a lower grade part requires additional testing to be performed in accordance with EEE-INST-002 to upgrade the part to level 2.

Parts selected from the GSFC Common Part Selection List (CPSL) or NASA Part Selection List (NPSL) for quality level 2 or better are preferred. All other EEE parts shall be selected, manufactured, processed, screened, and qualified, as a minimum, in the same manner as the nearest applicable quality level 2 device.

EEE-INST-002 contains value added testing for a number of parts listed in the CPSL and NPSL. The CPSL and NPSL are available at the following URLs, respectively: <http://cpsl.gsfc.nasa.gov>, and <http://nepp.nasa.gov/npsl>. These tests include PIND testing for EEE devices with internal cavities, 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.

11.4.3 Radiation Requirements for Part Selection

11.4.3.1 General

The developer shall ensure an appropriate radiation hardness assurance program is developed and conducted, through PCB and the GSFC Project Radiation Engineer (PRE), based on project requirements. The Parts Control Plan shall address all phases of the flight hardware development including the design, test, and production.

11.4.3.2 Specification of the Radiation Environment

The radiation environment for the mission has been specified (LDCM Radiation Environment Specification (TBS)) and shall be used for parts selection. This includes the trapped particle environment, galactic cosmic ray environment and solar particle event environment, and induced environments such as that caused by a radioisotope thermal generator.

11.4.3.3 Radiation Transport Analysis

When deemed necessary, the developer shall perform transport calculations for the incident radiations for shielding appropriate for the mission of interest using established codes.

11.4.3.4 Evaluation of Radiation Effects in Parts

The developer shall select all parts ensuring that they perform their function in their intended application in the predicted radiation environment including the applicable Radiation Design Margin (RDM). The radiation environment causes the following three main degradation effects that must be accounted for all active parts selection:

- **Total Ionizing Dose (TID)**, including Enhanced Low Dose Rate (ELDR) effects. Parts shall be selected to ensure their adequate performance in the application up to a dose of 2x the expected mission dose.
- **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) shall be avoided. If performance demands the use of an SEL susceptible part, measures shall be implemented to ensure that SEL induced damage (both prompt and latent) are mitigated and that the spacecraft's performance is not compromised. These measures must be approved by the developer Radiation Engineer (RE) and PPE, along with GSFC Project Radiation Engineer (PRE) and GSFC PPE before the part can be added to the PAPL.
- **Displacement Damage**, Parts shall be able to withstand the displacement damage induced by high energy protons, to twice the fluence expected in the predicted MMS environment.

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

11.4.4 Custom or Advanced Technology Devices.

Devices such as custom hybrid microcircuits, detectors, Application Specific Integrated Circuits (ASICs), and Multi Chip Modules (MCMs) shall also be subject to parts control and include a design review by the PCB appropriate for the individual technology. The design review shall include element evaluation to assure each element's reliability, (review shall 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, metals 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 PCB. These specifications shall fully describe the item being procured and shall include physical, mechanical, environmental, electrical test requirements, and quality assurance provisions necessary to control manufacture and acceptance. Screening requirements designated for the part can be included in the procurement specification. Test conditions, burn-in circuits, failure criteria, and lot rejection criteria shall 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 closest military part specification and/or GSFC EEE-INST-002.

11.4.5 Plastic Encapsulated Microcircuits (PEMs)

The use of Plastic Encapsulated Microcircuits is discouraged. However, when use of PEMs is necessary to achieve unique performance requirements that can not be achieved by 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 plastic encapsulated parts to assure that all aspects of EEE-INST-002 have been met.

11.4.6 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 as indicated 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.

11.4.7 Parts Approved on Prior Projects

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 LDCM. 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 LDCM). Such candidate parts shall be evaluated by the PCB for compliance to current Project requirements by determining that:

1. No changes have been made to the previously approved NSPAR, Source Control Drawing (SCD) or supplier list.
2. All stipulations cited in the previous NSPAR approval have been implemented on the current flight lot, including performance of any additional testing.
3. The previous project’s parts quality level is identical to the current project.
4. No new information has become available which would preclude the use of the previously approved part in a high reliability space flight application.

11.4.8 Parts Used in Off-the-Shelf Assemblies

Units or assemblies that are purchased as “off-the-shelf” hardware items shall be subjected to an evaluation of the parts used within them. The parts shall be evaluated for screening compliance to EEE-INST-002, established reliability level, and include a radiation analysis. Units may be required to undergo modification for use of higher reliability parts or Radiation hardened parts. Modifications such as additional shielding for radiation effectiveness or replacing radiation-soft parts for radiation-hardened parts may be required and shall be subject to PRE approval as part of the PCB approval activities.

11.5 PART ANALYSIS

11.5.1 Destructive Physical Analysis

A sample of each lot date code of Field Programmable Gate Arrays (FPGAs), hybrid microcircuits, microcircuits, oscillators, and semiconductor devices shall 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. The PCB on a case-by-case basis shall consider variation to the DPA sample size requirements, due to part complexity, availability or cost.

11.5.2 Failed EEE Parts

The developer shall have a method in place to report all EEE component failures during EEE part screening and qualification; during qualification and acceptance testing of flight hardware - beginning with the first application of power at the subassembly level continuing through, unit, subsystem, and system levels. 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 for review and approval.

11.5.3 Failure Analysis

When a component part Failure Analysis (FA) is necessary to support a Failure Review Board (FRB) activity, the developer shall prepare a part Failure Analysis Report. The Developer 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 as a minimum, provide the following information:

- 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 a secondary (collateral) failure (caused by another failure in the circuit and not a failure on its own merit.)
- The results of the failure analyses conducted and the nature of the rework/retest/corrective action taken in response.

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 pertinent to the failure mechanism. The FRB shall achieve a timely resolution and closure of each failure incident and shall document the findings.

11.6 ADDITIONAL REQUIREMENTS

11.6.1 Parts Age Control

All parts procured with date codes greater than five (5) years from the date of manufacture to date of procurement shall be subjected to a re-screen and sample DPA per PCB recommendation. Alternate test plans may be used as approved by the PCB on a case-by-case basis. Parts taken from user inventory older than 5 years, do not require re-screen provided they have been properly stored and use has been approved by the PCB. Proper storage is defined as maintaining the parts within their rated temperature range and 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). Parts over 10 years old from the date of manufacture to the date of procurement shall not be procured.

11.6.2 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 developer's PCP for approval.

11.6.3 GIDEP 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. The review process shall continue from delivery up to launch.

11.6.4 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.

All EEE parts shall be inspected to determine that there are no prohibited metals on any EEE part. An alternate method to ensure that no prohibited metal is used on EEE parts may be employed with PCB approval.

11.6.5 Traceability

The developer shall utilize traceability database(s) that shall provide the capability to retrieve historical records of EEE parts from initial procurement and receipt through storage, kitting, assembly, test, and final acceptance of the deliverable product. Also, the database shall permit the traceability to the procurement document and shall provide for:

- Cross-referencing and traceability of part manufacturer and date code to the assembly traveler or production plan.
- The storage of the accumulated data records.

All flight EEE parts shall be traceable to the date code or manufacturer's inspection lot, wafer lot (where applicable) and shall be maintained throughout manufacturing for each deliverable item.

11.6.6 ESD Control

The developer shall ensure that storage areas, laboratories, and work areas that receive, distribute, assemble, disassemble, handle, test or repair electrostatic discharge sensitive (ESDS) equipment are inspected and ESD- certified for proper equipment and handling procedures in accordance with Section 10.6 of this MAR.

11.7 PARTS LISTS

The developer shall develop and maintain a Parts Identification List (PIL), Project Approved Parts List (PAPL) and As-Designed Parts List (ADPL) (CDRL SA-20) for the duration of the project. Parts must be approved for listing on the PAPL before initiation of procurement activity. Long Lead items shall be identified on the PIL and have conditional approval from the PCB before procurement.

11.7.1 Parts Identification List (PIL)

The PIL shall list all parts proposed for use in flight hardware. The PIL is prepared from design team inputs or supplier inputs, to be used for presenting and tracking candidate parts to the PCB. The PIL shall include as a minimum the following information: Part type, Manufacturer's generic part number, part description, manufacturer, procurement specification, comments and FSC.

11.7.2 Project Approved Parts List (PAPL)

The PAPL (CDRL SA-20) shall list only approved parts for flight hardware, and shall be the combined listing of all parts submitted through Parts Identification Lists 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 PAPL across various systems and subsystems.

11.7.3 As-Designed Parts List (ADPL)

The developer PPE shall establish an As-Designed Parts List (ADPL) (CDRL SA-20) as soon as practical after the preliminary release. The GSFC PPE shall maintain a copy in the GSFC Parts Database, and will work with the design teams to keep the list(s) current.

11.7.4 As-Built Parts List (ABPL)

An As-Built Parts List (ABPL) (CDRL SA-20) shall also be prepared and submitted to the LDCM project by the Developer PPE. The ABPL is a final compilation of all parts as installed in flight equipment, with additional "as-installed" part information such as manufacturer name, CAGE code, Lot-Date Code, part serial number (if applicable). 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.

11.8 DATA REQUIREMENTS

11.8.1 General

Upon request, attributes summary data shall be provided to the Project Parts Engineer for all testing performed as applicable. The developer shall ensure that variable data (read and record) is recorded for initial, interim and final electrical test points as applicable. The developer shall provide this data to GSFC upon request.

For flight lots with samples subjected to Radiation Lot Acceptance Testing (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 as applicable.

Each developer and supplier shall perform, or be responsible for the performance of applicable incoming inspections to ensure that products meet the requirements of the procurement specification.

11.8.2 Retention of Data, Part Test Samples and Removed Parts

The developer shall have a method in place for the 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, as needed. 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. Data shall be retained for the useful life of the spacecraft, unless otherwise permitted by the PCB. All historical quality records and data required to support these records shall be retained for a period of 5 years and shall be provided to GSFC upon request.

Chapter 12.0 Materials, and Processes Requirements

12.1 GENERAL REQUIREMENTS

The developer shall plan and implement a comprehensive Materials and Processes Control Program (MPCP) at the design stage of the hardware to help ensure the success and safety of the MMS mission by the appropriate selection, processing, inspection, and testing of the materials and lubricants for use in flight hardware.

12.2 MATERIALS AND PROCESSES CONTROL PLAN

The developer shall provide a Materials and Processes Control Plan (MPCP) (CDRL SA-21) describing the approach and methodology for implementing the Materials and Processes Control Program. The MPCP shall also define the developer's criteria for materials and processes selection and approval based on this section.

12.3 MATERIALS SELECTION REQUIREMENTS

The developer shall, when selecting materials and lubricants, consider potential problem areas such as radiation effects, thermal cycling, stress corrosion cracking, galvanic corrosion, hydrogen embrittlement, lubrication, contamination, composite materials, atomic oxygen, useful life, vacuum outgassing, toxic offgassing, flammability and fracture toughness, as well as the properties required by each material usage or application.

The developer shall provide a Material Usage Agreement (Figure 12-1) or Stress Corrosion Evaluation Form (Figure 12-2) for each material that is not used in a conventional application and/or does not meet the following selection criteria:

- a. Hazardous materials requirements, including flammability, toxicity and compatibility as specified in AFSPCMAN 91-710, and NASA-STD-6001, Flammability, Odor, Off-gassing and Compatibility Requirements;
- b. Vacuum outgassing requirements as defined below (7.3.3);
- c. Stress corrosion cracking requirements as defined in MSFC-STD-3029, Design Criteria for Controlling Stress Corrosion Cracking.

12.3.1 Fasteners

The developer shall comply with the procurement documentation and test requirements for flight hardware and critical ground support equipment (GSE) fasteners (unless the GSE is qualified by proof-testing) outlined in 541-PG-8072.1.2, Goddard Space Flight Center Fastener Integrity Requirements (formerly GSFC S-313-100). (For a copy of 541-PG-8072.1.2, use the following hyperlink <http://gdms.gsfc.nasa.gov/gdms/plsql/masterlist.menu>.) The developer shall provide material test reports for fasteners for review upon request.

The developer shall ensure that fasteners made of plain carbon or low alloy steel are protected from corrosion. When plating is specified, it shall be compatible with the space environment.

On steels harder than RC 33, plating shall be applied by a process, which is not embrittling to the steel.

12.3.2 Flammability and Toxicity

The developer shall ensure that materials meet the appropriate range safety requirements for usage of hazardous materials.

12.3.3 Vacuum Outgassing

The developer shall determine material vacuum outgassing in accordance with ASTM E-595. 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 acceptable for use in a vacuum environment.

12.3.4 Shelf-Life-Controlled Materials

The developer shall control polymeric materials that have a limited shelf life by a process that identifies the start date (manufacturer's processing, 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, rosin core solder, lubricated bearings and paints shall be included. The use of materials with expired date code requires a demonstration, by means of appropriate tests, that the properties of the materials have not been compromised for their intended use.

12.4 AS-DESIGNED/AS-BUILT MATERIALS AND PROCESSES LIST (M&P LIST)

The developer shall maintain an As-Designed/As-Built Materials and Processes (M&P) List (CDRL SA-22) of all materials and processes planned for use in flight hardware. The lists shall include a Polymeric Materials and Composites Usage List, an Inorganic Materials and Composites Usage List, a Lubrication Usage List, and a Materials Process Utilization List.

12.4.1 Polymeric Materials

A polymeric materials and composites usage list (Figure 12-3), or equivalent, shall be prepared and submitted as a part of the M&P Lists.

12.4.2 Inorganic Materials

An inorganic materials and composites usage list (Figure 12-4), or equivalent, shall be prepared and submitted as a part of the M&P Lists. In addition, the developer may be requested to submit supporting applications data. The criteria specified in MSFC-STD-3029 shall be used to determine that metallic materials meet the stress corrosion cracking (SCC) criteria. An MUA (Figure 12-1) and SCC evaluation (Figure 12-2), or the developer's equivalent forms, shall be submitted for GSFC LDCM Project to review for each material usage that does not comply with the MSFC-STD-3029 SCC requirements.

12.4.3 Lubrication

A lubrication usage list (Figure 12-5), or equivalent, shall be prepared and submitted as a part of the M&P Lists. Also, supporting applications data shall be submitted, upon request.

Lubricants shall be selected for use with materials on the basis of 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 effects.

All lubricated mechanisms shall be qualified by life testing; or heritage of an identical mechanism used in identical applications.

12.4.4 Process Utilization list

A material process utilization list (Figure 12-6), or equivalent, shall be prepared and submitted as a part of the M&P Lists. Manufacturing processes (e.g., lubrication, heat treatment, welding, and chemical or metallic coatings) shall be carefully selected to prevent any unacceptable material property changes that could cause adverse effects of materials applications.

FIGURE 12-1: MUA

MATERIAL USAGE AGREEMENT			USAGE AGREEMENT NO.:			PAGE OF	
PROJECT:		SUBSYSTEM:		ORIGINATOR:			ORGANIZATION:
DETAIL DRAWING	NOMENCLATURE			USING ASSEMBLY		NOMENCLATURE	
MATERIAL & SPECIFICATION				MANUFACTURER & TRADE NAME			
USAGE	THICKNESS	WEIGHT	EXPOSED AREA	ENVIRONMENT			
				PRESSURE		TEMPERATURE	MEDIA
APPLICATION:							
RATIONALE:							
ORIGINATOR:				PROJECT MANAGER:			DATE:

FIGURE 12-2: STRESS CORROSION EVALUATION FORM

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: _____

SPACECRAFT		SYSTEM EXPERIMENT		GSFC TO			
DEVELOPER/DEVELOPER		ADDRESS		DATE			
PREPARED BY		PHONE		DATE PREPARED			
GSFC MATERIALS EVALUATOR		PHONE		DATE RECEIVED			
		OR OTHER SPEC. NO.		DATE EVALUATED			
ITEM NO.	MATERIAL DESCRIPTION ¹⁾	QSN ²⁾	APPLICATION ³⁾	EXPECTED EXPOSURE ⁴⁾	S.C.C. TABLE NO.	M/U NO.	NDE METHOD
<p>NOTES:</p> <ol style="list-style-type: none"> 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. Give materials name, identifying number manufacturer. <p>Example:</p> <ol style="list-style-type: none"> Aluminum, 6061-T6 Electroless nickel plate, Example: Ni 410, Electroless, Inc. Fused silica, Corning 7940, Corning Glass Works 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. <p>Example:</p> <ol style="list-style-type: none"> Heat-treated to Rockwell C 60 hardness, gold electroplated, brazed. Surface coated with vapor deposited aluminum and magnesium fluoride Cold worked to full hard condition, TIG welded and electroless nickel-plated. Give details of where on the spacecraft the material will be used (component) and its function. <p>Example: Electronics box structure in attitude control system, not hermetically sealed.</p> <p>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 a group.</p> <p>Example: T/V: -20C/+60C, 2 weeks, 10E-5 torr, Ultraviolet radiation (UV) Storage: up to 1 year at room temperature Space: -10C/+20C, 2 years, 150 miles altitude, UV, electron, proton, Atomic Oxygen</p>							



FIGURE 12-5: LUBRICATION USAGE LIST

LUBRICATION USAGE LIST		SPACECRAFT _____		SYSTEM EXPERIMENT _____		GSFC TO _____	
DEVELOPED/DEVELOPER _____		ADDRESS _____		DATE _____		DATE _____	
PREPARED BY _____		PHONE _____		DATE PREPARED _____		DATE _____	
GSFC MATERIALS EVALUATOR _____		PHONE _____		DATE RECEIVED _____		DATE EVALUATED _____	
ITEM NO.	COMPONENT TYPE, SIZE	COMPONENT MANUFACTURER & MFG. IDENTIFICATION	PROPOSED LUBRICATION AMT. OF LUBRICANT	TYPE & VISC. OF WAX	SPEED, TEMP. OF OPERATION	TYPE OF LOADS & AMT.	OTHER DETAILS
<p>NOTES</p> <p>(1) Ball bearing, SB - skew bearing, G - gear, SS - sliding surfaces, SEC - sliding electrical contacts. Give generic identification of materials used (e.g., 440C steel pipe).</p> <p>(2) CLR - continuous unidirectional rotation, CV - continuous oscillation, IR - intermittent rotation, IO - intermittent oscillation, SO - small oscillation, (<30°), LO - large oscillation (>30°), CS - continuous sliding, IS - intermittent sliding. No. of start cycles: $A:1-10^7$, $B:10^2-10^4$, $C:10^4-10^6$, $D:>10^6$</p> <p>(3) Speed: RPM - rev./min., OPM - oscillation/min., VS - variable speed RPM - constant. (Specify applications). Temp. of operation, min. & max. °C. Atmosphere: vacuum, air, gas, sealed or unsealed & pressure.</p> <p>(4) Type of load: A - axial, R - radial, T - tangential (gear loads). Give amount of load.</p> <p>(5) If B&B, give type and material of ball cage and number of balls and specified ball groove and ball finish. If G, give surface treatment and hardness. If SB, give dia. of bore and width. If bearing available is limited, give approx. ϕ dia.</p>							

GSFC 18-59C 3/78



FIGURE 12-6: MATERIALS PROCESS UTILIZATION LIST

MATERIALS PROCESS UTILIZATION LIST					
SPACECRAFT _____		SYSTEM/EXPERIMENT _____			
DEVELOPER/DEVELOPER _____			ADDRESS _____		
PREPARED BY _____			PHONE _____		DATE PREPARED _____
GSFC MATERIALS EVALUATOR _____			PHONE _____		DATE RECEIVED _____ DATE EVALUATED _____
ITEM NO.	PROCESS TYPE ⁽¹⁾	DEVELOPER SPEC. NO. ⁽²⁾	MIL., ASTM, FED. OR OTHER SPEC. NO.	DESCRIPTION OF MAT'L PROCESSED ⁽³⁾	SPACECRAFT/EXP. APPLICATION ⁽⁴⁾
<p>NOTES</p> <p>(1) Give generic name of process, e.g., anodizing (sulfuric acid).</p> <p>(2) If process is proprietary, please state so.</p> <p>(3) Identify the type and condition of the material subjected to the process. E.g., 6061-T6</p> <p>(4) Identify the component or structure of which the materials are being processed. e.g., Antenna dish</p>					

GSFC 18-59D 3/78

DRAFT

Chapter 13.0 GROUND DATA SYSTEMS ASSURANCE REQUIREMENTS

13.1 GENERAL

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.

13.2 QUALITY MANAGEMENT SYSTEM

QMS related requirements are discussed in Chapter 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 (quality 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. Quality 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.

13.3 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 lifecycle. All changes to the GDS requirements, including those generated both internally and externally, shall be managed by the developer's Configuration Control Board (CCB) process and reviewed/approved as applicable by GSFC.

13.4 REVIEWS

The developer shall implement a program of engineering reviews (peer reviews) throughout the development lifecycle 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.

13.5 ASSURANCE ACTIVITIES

The developer shall perform various assurance-related activities throughout the development lifecycle to ensure that the GDS and its components meet GDS requirements. The developer shall initiate these activities as early in the development lifecycle 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 lifecycle and the developer shall conduct these activities throughout the entire lifecycle. These activities include but are not limited to Planning, Tracking and Oversight.

13.5.1 Concept Phase

Specific assurance-related activities that the developer shall perform during the concept phase include but are not limited to the following:

- Tradeoff and evaluation studies and/or prototyping efforts to provide insight into the feasibility of GDS components meeting the operational concept, constraints and preliminary requirements.
- Define and document criteria used to perform tradeoff and evaluation studies and maintain all results from these studies for GSFC review.
- Participation in a system requirements reviews.

13.5.2 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.
- Document trade studies and analyses performed to aid in deciding which requirements to allocate to hardware, software and other components. When a system-level requirement is

allocated to more than one configuration item (CI), a process is used to assure that the lower-level requirements taken together satisfy the system-level requirement.

- 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.
- Ensure that the systems analysis and allocation methodology is compatible with other methodologies adopted on the project.
- 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 lifecycle 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.

13.5.3 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):

- Select and document an engineering development lifecycle model consistent with the program requirements and needs. The rationale for selecting the lifecycle development models and methods shall be recorded and maintained.
- Establish and maintain the computer system architecture (hardware, software and other components), for determining the nature and number of the configuration items, and for maintaining traceability of the architecture to requirements. This process shall define the relationships between GDS architecture components (hardware, software, etc) including the system-level component hierarchy and control structure and the operational (human) interface as applicable.
- Maintain a process to define, maintain, and document interfaces (both internal and external) within the architecture.
- Evaluate how suitable the GDS architecture is for implementing all of the requirements, as well as how the design constraints are satisfied. The developer shall identify, document and maintain criteria used to perform any architecture evaluations. Suitable development/project personnel shall participate and support these evaluation efforts.

- Evaluate the design based on the use of risk reduction techniques, such as the creation of models and prototypes (proofs, benchmarks) as necessary.
- Periodically reassess the adequacy of the GDS architecture over the development cycle. The developer shall identify, document and maintain criteria that are used to provide data to determine whether to stay with the original design or change.
- As requirements change, perform a review of the GDS architecture design for flexibility to adapt to new requirements, and (as necessary) updates, the ground data system architecture design.
- Review all architectural changes and their impact on design margins (such as memory, throughput, bus loading and data latency) as well as cost and schedule baselines prior to implementation. Any proposed change to the GDS architecture design shall be subject to GSFC review/approval.
- Document and maintain the rationale of all major systems engineering decisions and where applicable implement a process to arbitrate contention across trade-off studies for utilization of system-level resources and reserves.
- Conduct reviews and appropriate tests at the end of each phase of the development process 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.
- Conduct design walkthroughs and reviews.

13.5.4 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 phase of the development process 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.
- Conduct configuration reviews, Functional Configuration Audits (FCAs) and Physical Configuration Audits (PCAs) to define, document and ensure the configuration of the GDS and its components.

13.5.5 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). As necessary, 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 is not limited to the following:
 - Number of system builds planned and when they will occur.
 - 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 lifecycle, 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 lifecycle to include the status (pass, fail, deferred, etc) of each requirement throughout the testing phases and various testing activities.
- Document all test results in a test report. 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.
- Define and document a transition process/plan to progress from the test environment to the operations and maintenance environment.

- 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 abnormal/erroneous condition testing as appropriate.
- Maintain a process for determining the level of test for safety critical GDS components. The developer shall develop test procedures to ensure that all safety critical GDS components are tested at and beyond the systems limits, with abnormal/erroneous conditions, as well as all transition points (e.g., mode to mode). The developer shall execute these test procedures for all safety critical GDS components.
- Conduct reviews and appropriate tests at the end of each phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data.
- 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. s/c, s/c data tape, engineering test unit or s/c 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.
- Conduct reviews and appropriate tests at the end of each phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data.

13.5.6 Operations and Maintenance Phase

Specific assurance-related that the developer shall perform during the operations and maintenance phase include but are not limited to the following (note: some of these activities may be performed prior to this phase as applicable):

- Generate and deliver to GSFC formal acceptance data delivery packages identifying the contents of the delivery and any associated metadata/artifacts describing the delivery and its contents.

For those GDS instances where hardware is delivered, contents of the data delivery package shall include but is not limited to the following information:

- a. As-Built configuration list.
 - b. List of parts used.
 - c. List of materials and processes used.
 - d. Test logbook including total operating time and cycle records.
 - e. List of open items (i.e., nonconformances, etc) with reasons for items being open and appropriate authorization/approvals/waivers.
 - f. Listing and status of all identified Limited-Life items.
 - g. Trend data.
 - h. Test results and verification success criteria.
 - i. Known problems and workarounds.
- For those GDS instances where software is delivered, contents of the data delivery package shall include but is not limited to the following information:
 - a. Software Delivery Letter.
 - Description of delivery contents
 - Build instructions.
 - Special operating instructions.
 - List of resolved anomaly reports and change requests.
 - List of unresolved anomaly reports and change requests.
 - Copy of resolved anomaly reports and change requests.

- Copy of unresolved anomaly reports and change requests.
 - Matrix of requirements addressed by this release, including waivers for those requirements not met as appropriate.
 - Release history summary matrix.
 - Inventory of the delivered media.
 - List of changes to documentation associated with this release.
 - Verification success criteria
 - Known problems and workarounds.
- b. Software Delivery Media.
- c. Accompanying Documentation

13.5.7 Activities Performed throughout the Lifecycle

13.5.7.1 Planning, Tracking and Oversight

- The developer shall define and document a Management Program to include planning, tracking and oversight activities for the project/program in a development plan, see DID 5-1 for guidance.
- The developer shall ensure that periodic and appropriate coordination among developers, acquisition organizations, users, maintainers, testers, QA and customers, regarding user needs, acquisition organization resources, technology status, and GDS requirements occurs throughout the development lifecycle.
- The developer shall ensure and maintain a system engineering process (as appropriate) that emphasizes an integrated product development approach. This approach shall define systems engineering interfaces with other engineering interfaces and disciplines with the development activities, as well as the interfaces between the system and subsystem developers and/or subcontractors/COTS vendors. The developer shall ensure and maintain a process to manage, provide an escalation path for, and resolve conflicts regarding intergroup issues, including system-level issues that arise internally or with subcontractors/COTS vendors. The developer shall identify and track critical dependencies between development groups participating in development activities.
- The developer shall utilize support tools that are compatible with other tools used by other project members to facilitate the communication, exchange and sharing of data.
- The developer shall identify and select metrics to be collected and analyzed on a routine basis to ensure development and management activities are proceeding per customer requirements. Metrics shall be based upon the program's defined system engineering process.
- The developer shall define the specific measurement data to be collected, their precise definitions, the intended use and analysis of each measurement and the process control points at which they will be collected and reported.
- The developer shall identify and maintain requirements for metrics, define variance thresholds, which when exceeded require corrective actions.

- The developer shall ensure that the measurement program is integrated with the program's development process across the lifecycle and any teaming/subcontracting arrangements.
- The developer shall maintain a quality plan that serves as the basis for the project's activities for quality management. The quality goals for the GDS and its associated components shall be defined, monitored, and revised throughout the lifecycle. Quality goals shall be allocated appropriately to the subcontractors delivering products and/or GDS components to the project whenever applicable.
- The project's quality plan shall contain provisions to ensure that quality is built into the GDS and its associated components. The plan shall identify points in the lifecycle process where quality is measured. The plan shall identify methods for analyzing quality measurements, for evaluating whether they meet customer's needs, and for determining the necessary corrective actions.
- The developer shall maintain/possess a QA organization/entity that is assigned the responsibility to monitor the development process, and the associated components/products. QA shall interface with all relevant disciplines participating in the lifecycle activities including engineering, configuration management and testing. The QA group is empowered to effect changes to the program when quality goals are not being met.
- The developer shall follow a written QA plan for measuring and monitoring the performance of the program's defined management and development processes. The developer shall verify adherence to the defined development and management processes. The developer shall perform audits on designated work products to verify compliance with quality goals, and adherence to the applicable standards and requirements.

13.6 GFE, COTS, EXISTING AND PURCHASED SOFTWARE

- If the developer will be provided software as GFE, 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.
- The developer shall be responsible for ensuring that these components meet all applicable standards, including those for design, code and documentation, or for securing a GSFC project waiver to those standards.
- The developer shall be required to submit documentation providing indication of suitability for use and compliance to all applicable requirements and standards.
- 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 defined by the project and its CCB procedures and will be subject to GSFC review.

13.6.1 COTS Management

- The developer shall identify and maintain traceability of GDS requirements satisfied by COTS products/components.
- The developer shall conduct trade studies to identify potential COTS products that may meet GDS requirements.
- The developer shall identify and maintain criteria for COTS selection.

- The developer shall document the rationale/justification for the selection of all COTS components contained within the GDS.
- The developer shall maintain a CM program for all COTS products/components of the GDS.
- The developer shall maintain a COTS management plan for all COTS products/components of the GDS.
- The COTS management plan shall include and address the adequacy of existing COTS products/components in meeting or exceeding GDS requirements, processes utilized to ensure COTS updates/upgrades are routinely assessed and implemented based upon a documented criteria, etc.
- The developer shall demonstrate and document the fulfillment of GDS requirements by COTS products/components via the RVM.

13.7 REUSE REQUIREMENTS

- The developer shall maximize future reuse potential of new developed system and software components within the constraints of the system cost, schedule and performance baselines.
- The developer shall identify, assess and document lifecycle impact of reuse-related decisions, including the choice of computer languages, processors, architectures, environments, the development of reusable assets and the maintenance of re-use repositories.

13.8 DEFECT PREVENTION REQUIREMENTS

- The developer shall develop and maintain a program/plan for defect prevention activities.
- The developer's program/plan shall at a minimum, include identification of defect causes and assessments for potential process improvement opportunities. The developer shall conduct causal analysis meetings as appropriate. Data on defects as identified in peer reviews, document reviews and testing shall be collected and analyzed by the developer. The developer shall identify, prioritize and systematically eliminate common causes of defects based upon their defect prevention program/plan.
- The developer shall revise development and management processes as a result of defect prevention actions as applicable.
- The developer shall document and track defect prevention data across entities coordinating defect prevention activities. The developer shall provide feedback on the status and results of the organization and program's defect prevention activities to project personnel on a periodic basis.

13.9 DATABASES

- The developer shall maintain a process and procedures for database development. The process shall include activities such as internal reviews, walkthroughs, statusing, test and discrepancy resolution.
- The developer shall ensure that the database development processes and procedures are compatible with the selected database methodology.
- The developer shall utilize a process for the verification and validation of the database system.

- The developer shall ensure that system/software releases and database releases are configured with one another.
- The developer shall test the interface between the software and Database Management System (DBMS) tested.
- 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.
- The developer shall ensure that appropriate security measures are implemented on the database system and on the data contained within the database system.

13.10 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 lifecycle. 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.

13.11 ELECTROMAGNETIC COMPATIBILITY CONTROL

For GDS components subject to electromagnetic compatibility problems, the developer shall submit an Electromagnetic Compatibility Control (EMC) test plan in accordance with the contract schedule that identifies an overall implementation of an effective EMC test program. The test plan shall include test requirements that will assure compatibility within each element, within the project as a whole, and within the project's facilities. It shall describe any special testing requirements and the content of EMC sections of applicable Interface Control Documents (ICDs). The EMC test plan and the activities described within it shall comply with the requirements found in MIL-STD-461, "Electromagnetic Emission and Susceptibility Requirement for Control of Electromagnetic Interference", as applicable.

13.12 RELIABILITY AND AVAILABILITY

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

- The developer shall define, measure, control and report on reliability in all lifecycle phases as appropriate. The developer shall implement corrective actions whenever reliability related requirements are not being satisfied.
- The developer shall allocate basic reliability and mission reliability requirements to the GDS architecture component level (at which failures are postulated), necessary to identify redundancy. The developer shall ensure that reliability requirements are used to establish baseline requirements against which the design alternatives are evaluated. Requirements consistent with the allocations shall be imposed on any subcontractors, suppliers and/or COTS vendors whenever appropriate.
- The developer shall assure that equipment and components obtained from subcontractors, suppliers and/or COTS vendors meet allocated requirements and if not, such deficiencies shall be report to GSFC.
- The developer shall develop reliability predictions for the GDS and its components. These models and predications shall reflect applicable experience from previous projects and/or similar GDS components and shall be revised/maintained throughout the lifecycle as pertinent data becomes available. These models shall be documented, accessible for GSFC review and used continually throughout the design process. These reliability models shall be used to augment system engineering tradeoff studies. Appropriate prediction techniques are described in Chapter 4.
- The developer shall develop and document analyses to determine possible modes of failure and their effects on the GDS and its components. Appropriate analysis techniques are described in Chapter 4.
- The developer shall perform reliability evaluation on the GDS and its components via the collection of failure and time data throughout the lifecycle. Appropriate evaluation techniques are described in Chapter 4.

13.12.1 Reliability Acceptance Testing

The GDS and/or its components shall be subjected to a failure free acceptance test by government personnel and its representatives, as required. The length of the test will be as specified in the contract; for example, in the range from 300 to 1,000 hours. The developer shall provide the resources to create the test software, hardware and test data; as well as support testing operations, analyze results and make corrections as required.

The general guidelines to be followed include the following:

- a. The developer shall certify in writing that the system is installed and ready to use, and shall provide documentation of a successful system checkout performed which demonstrates that the system, including hardware and software components, is in an acceptable operating condition. The system will then be turned over for testing by an Acceptance Test team.
- b. If the equipment operates failure free in accordance with the specification during the specified performance period the equipment shall be deemed to have met the standard of performance.

- c. If a failure occurs, the test shall be terminated and the developer shall be responsible for determining the cause of the failure. The equipment shall then be returned to working condition and resubmitted for test.
- d. If the equipment fails to meet the standard of performance after the specified number of attempts, because of recurring failures, the Technical Officer may, at his option, notify the Contracting Officer to require a replacement of said equipment or to terminate the contract in accordance with the provisions of the default clause of this contract.
- e. Operational use time for equipment is defined as the accumulated time during which the unit(s) is (are) in actual operation, including any interval of time between the start and stop of the central processing unit(s).
- f. In addition to any diagnostic programs provided by the developer, the government may use additional test programs developed by the team with technical assistance from the developer, as required.

The developer shall provide test procedures and test reports in accordance with the contract schedule. The test procedures shall make full use of benchmark and standard system diagnostics to verify compliance to performance requirements including interfaces. Documentation on how to run the test(s) and interpret the results will be specified in the procedures.

13.13 MAINTAINABILITY REQUIREMENTS

Maintainability assurance requirements for the GDS and associated components shall include the following:

- The developer shall define and evaluate the effort, cost and equipment required to support/maintain the GDS and its components.
- The developer shall define, measure, control and report on maintainability in all lifecycle phases as appropriate. The developer shall implement corrective actions whenever maintainability related requirements are not being satisfied.
- The developer shall allocate maintainability requirements to the GDS architecture component level as appropriate. The developer shall ensure that maintainability requirements are used to establish baseline requirements against which the design alternatives are evaluated. Requirements consistent with the allocations shall be imposed on any subcontractors, suppliers and/or COTS vendors whenever appropriate.
- The developer shall assure that equipment and components obtained from subcontractors, suppliers and/or COTS vendors meet allocated requirements and if not, such deficiencies shall be report to GSFC.
- The developer shall develop maintainability predictions for the GDS and its components. These models and predications shall reflect applicable experience from previous projects and/or similar GDS components and shall be revised/maintained throughout the lifecycle as pertinent data becomes available. These models shall be documented, accessible for GSFC review, and used continually throughout the design process. These maintainability models shall be used to augment system engineering tradeoff studies. Appropriate prediction techniques are described in Chapter 4.

- The developer shall perform maintainability evaluation/demonstration tests on the GDS and its components to verify that all preventive and corrective maintenance activities, such as system and data level backups, can be successfully executed. Maintainability demonstration shall be conducted in the operational environment as available, or an environment that duplicates the operational environment as closely as possible. To the maximum extent possible, operators, technicians, system and/or database administrators of the system shall perform the maintenance actions during the maintainability demonstration.

13.14 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 NPG 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-8719.13 “NASA Software Safety Standard”. *See section 5.2.2 of this document for software safety related items.*
- The developer shall establish and identify procedures and instructions, which will be used to execute all system safety analyses. The developer shall perform system safety analyses assuring that:
 - a. Safety is designed into the product; known hazardous conditions that cannot be eliminated through equipment design or operational procedures are controlled or reduced to an acceptable level. Residual hazards shall be tracked with their severity status and provided to NASA on a periodic basis.
 - b. Results of previous trade studies and analyses are considered.
 - c. Other related analyses, such as Failure Modes and Effects and Criticality Analysis (FMECA), are considered to preclude duplication of analytical work.
- All safety-related analyses, studies and assessments shall be accessible for GSFC review.

Chapter 14.0 Applicable Documents List

<u>DOCUMENT</u>	<u>DOCUMENT TITLE</u>
None	Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (Available at http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf)
None	NASA Parts Selection List (Available at http://nepp.nasa.gov/npsl)
461-RQMT-002	LDCM Mission Requirements Document
461-RQMT-0005	LDCM Observatory/Spacecraft Requirements Document
461-XXX	LDCM Project Plan (To be written)
AFSPCMAN 91-710	Range Safety User Requirements
ANSI/ISO/ASQ Q9001-2000	American National Standard Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation and Servicing
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).
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
GSFC-STD-7000	General Environmental Verification Specification (GEVS) for GSFC 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, Qualification, and Derating
IEEE 730-2002	IEEE Standard for Software Quality Assurance Plans
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
IPC A-600	Guidelines for Acceptability of Printed Boards
ISO 17025	General Requirements for the Competence of Testing and Calibration Laboratories
MIL-STD-461	Electromagnetic Emission and Susceptibility Requirement for Control of Electromagnetic Interference
MSFC-HDBK-527	Material Selection List for Space Hardware Systems
MSFC-SPEC-522	Design Criteria for Controlling Stress Corrosion Cracking

MSFC-STD-3029	Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments
NASA RP-1124	Outgassing Data for Selecting Spacecraft Materials
NASA RP-1161	Evaluation of Multi-layer Printed Wiring Boards by Metallographic Techniques
NPD 8710.3	NASA Policy for Limiting Orbital Debris Generation
NPD 8720.1	NASA Reliability and Maintainability (R&M) Program Policy
NPD 8730.4	NASA Policy for Software Independent Verification and Validation
NPG 7120.5	NASA Program and Project Management Processes and Requirements
NPG 8715.3	NASA Safety Manual
NASA-STD-6001	Flammability, Odor, Off-gassing and Compatibility Requirements & Test Procedures for Materials in Environments that Support Combustion
NASA-STD 8719.13	NASA Software Safety Standard
NASA-STD-8729.1	Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program
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
NASA-STD-8739.8	NASA Software Assurance Standard
NASA-STD-7150.2	NASA Software Engineering Requirements
NPR 8715.3	NASA Safety Manual
NSS 1740.14	Guidelines and Assessment Procedures for Limiting Orbital Debris
S-311-M-70	Specification for Destructive Physical Analysis
541-PG-8072.1.2	GSFC Fastener Integrity Requirements
5405-048-98	Mechanical Systems Center Safety Manual

Chapter 15.0 Acronyms

ABPL	As-Built Parts List
ADPL	As-Designed Parts List
ANSI	American National Standards Institute
ASIC	Application Specific Integrated Circuits
ASQ	American Society for Quality
ASTM	American Society for Testing of Materials
BB	Ball Bearing
BGA	Ball Grid Array
CCP	Contamination Control Plan
CCR	Configuration Change Request
CDR	Critical Design Review
CDRL	Contract Delivery Requirements List
CIL	Critical Items List
CM	Configuration Management
CO	Continuous Oscillation
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-The-Shelf
CPSL	Common Parts Selection List
CPT	Comprehensive Performance Test
CRM	Continuous Risk Management
CS	Continuous Sliding
CSI	Contractor Source Inspection
CUR	Continuous Unidirectional Rotation
CVCM	Collected Volatile Condensable Mass
DID	Data Item Description
DoD	Department of Defense
DPA	Destructive Physical Analysis
EEE	Electrical, Electronic, and Electromechanical
EIA	Electronics Industry Alliance
ELV	Expendable Launch Vehicle
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
ETA	Event Tree Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
FOR	Flight Operations Review
FRB	Failure Review Board
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
G	Gear
GEVS	General Environmental Verification Specification

LDCM MAR

GFE	Government Furnished Equipment
GIDEP	Government Industry Data Exchange Program
GOTS	Government Off The Shelf
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
IEEE	Institute of Electrical and Electronics Engineers
IO	Intermediate Oscillation
IPC	Association Connecting Electronics Industries
IR	Intermediate Rotation
IS	Instrument Sliding
ISO	International Organization for Standardization
IV&V	Independent Verification and Validation
LDCM	Landsat Data Continuity Mission
LO	Large Oscillation
LPT	Limited Performance Test
LRR	Launch Readiness Review
MAPTIS	Materials and Processes Technical Information Service
M&P	Materials and Processes
MAR	Mission Assurance Requirements
MCM	Multi-Chip Module
MEB	GSFC Materials Engineering Branch
MLD	Master Logic Diagram
MOR	Mission Operations Review
MOTS	Modified Off-The-Shelf
MRB	Material Review Board
MSPSP	Missile System Prelaunch Safety Package
MUA	Materials Usage Agreement
NASA	National Aeronautics and Space Administration
NCR	Nonconformance Report
NPD	NASA Policy Directive
NPG	NASA Procedures and Guidelines
NPSL	NASA Parts Selection List
NRCA	Nonconformance Reporting and Corrective Action
NSS	NASA Safety Standard
OPM	Oscillations Per Minute
O&SHA	Operating and Support Hazard Analysis
OSSMA	Office of Systems Safety and Mission Assurance
PAPL	Project Approved Parts List
PCB	Parts Control Board
PCP	Parts Control Plan
PDR	Preliminary Design Review
PEM	Plastic Encapsulated Microcircuit
PER	Pre-Environmental Review
PFR	Problem/Failure Report
PG	Procedures and Guidelines
PHA	Preliminary Hazard Analysis

PIL	Parts Identification List
PMPCP	Parts, Materials and Processes Control Program
PPE	Project Parts Engineer
PPL	Preferred Parts List
PRA	Probabilistic Risk Assessment
PSR	Pre-Shipment Review
PWB	Printed Wiring Board
QCM	Quartz Crystal Microbalance
RE	Radiation Engineer
RFO	Request for Offer
RMP	Risk Management Plan
RPM	Revolutions Per Minute
SAM	(NASA/GSFC) Systems Assurance Manager
SB	Sleeve Bearing
SCC	Stress Corrosion Cracking
SCD	Source Control Drawing
SEC	Sliding Electrical Contacts
SEE	Single-Event Effects
SMA	Safety and Mission Assurance
SO	Small Oscillation
SOW	Statement of Work
SQA	Software Quality Assurance
SRO	Systems Review Office
SRR	Systems Requirements Review
SS	Sliding Surfaces
SSPP	System Safety Program Plan
STD	Standard
TID	Total Ionizing Dose
TIM	Technical Interface Meeting
TML	Total Mass Loss
TR	Torque Ratio
URL	Uniform Resource Locator
UV	Ultraviolet
V&V	Verification and Validation
VS	Variable Speed
VTL	Verification Tracking Log

Chapter 16.0 Glossary

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.”

Collected Volatile Condensable Material (CVCN): 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 that are capable of fulfilling the fit, form and functional requirements defined by performance specifications and engineering drawings.

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.

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 the test 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.

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.

Fault Tree Analysis (FTA): A Fault Tree Analysis is a qualitative technique to uncover credible ways that a (undesired) top event can occur. The results of the FTA are documented in a fault tree which is a graphical representation of the combination of faults that will result in the occurrence of undesired top event.

Flight Acceptance: See “Acceptance Tests.”

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 three major categories of hardware as follows:

- a. **Development Hardware:** Non-flight breadboard and/or engineering model hardware intended to demonstrate specific aspects of the feasibility, performance, or reliability of the flight hardware.
- b. **Prototype Hardware:** Hardware constructed using the same design, materials, and processes as the flight hardware but not intended for flight use. It is subject to a design qualification test program but it is not intended for flight.
- c. **Flight Hardware:** Hardware to be used operationally in space. It includes the following subsets:
 - (1) **Protoflight Hardware:** Flight hardware is intended to be 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.
 - (2) **Follow-On Hardware:** Flight hardware built in accordance with a design that has been (or is being) qualified either as prototype or as protoflight hardware for an environment equal or more severe than the current missions. Follow-on hardware is subject to a flight acceptance test program.
 - (3) **Spare Hardware:** Hardware that is not currently slated for flight use. It is subject to a modified flight acceptance test program (that has been adjusted as needed to compensate for the higher assembly level testing to which the spare unit may not have been tested) and is used to replace flight hardware that is no longer acceptable for flight.
 - (4) **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.

Hazard: An existing or potential condition that can result in, or contribute to, a mishap. The following types of hazards may be referenced with respect to this document::

(1) **Catastrophic:**

- i. 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
- ii. A condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission.

(2) **Controlled (Risk):** A condition where the likelihood of an occurrence or the severity of the associated undesirable event has been reduced to an acceptable level through the imposition of appropriate, readily implementable, verifiable controls resulting in minimal residual risk.

(3) **Critical:** A condition that may cause severe injury or occupational illness or major property damage to facilities, systems, or flight hardware.

Independent Verification and Validation (IV&V): Verification and validation performed by an organization that is technically, managerially, and financially independent. IV&V, as a part of Software Assurance, plays a role in the overall NASA software risk mitigation strategy applied throughout the life cycle to improve the safety and quality of software systems. In addition to performing a second check on the requirements traceability and general process as well as product reviews, IV&V is used to apply additional analyses to safety critical products.

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 spacecraft level). The assurance program includes the part level. Verification testing may also include testing at the assembly and subassembly levels of assembly; for test record keeping 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 spacecraft 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 spacecraft).
- 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 spacecraft 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.

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

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. It may also be considered a nonconformance when certain out-of-family conditions exist such that a characteristic or functional parameter differs sufficiently from expected, usual, or historical norms as to indicate a significant risk that the item will not perform as intended.

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.

Probabilistic Risk Assessment (PRA): Probabilistic Risk Assessment is a rigorous technical discipline used in complex technological applications to reveal design, operation, and maintenance vulnerabilities to enhance safety and to reduce costs.

Protoflight Testing: See “Hardware.”

Prototype Testing: See “Hardware.”

Qualification: See “Design Qualification Tests.”

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 op within specified limits.

Residual Risk: A risk that remains from a hazard after all mitigation and controls have been applied.

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

Risk: A risk is the combination of the probability that a project will experience an undesired event (e.g., safety mishap, environmental exposure, failure to achieve mission success criteria, cost overrun, schedule slippage, etc.) and the consequences, impact, or severity of the undesired event were it to occur.

Risk Management: Risk Management is a process wherein the project manager leads the project team in identifying, analyzing, planning, tracking, controlling, and communicating the risks and the actions to manage/control them. This process requires effective communication the team and with management and with customers. Risk management is driven by established success criteria and is a continuous, iterative process to manage risk in order to achieve safety and mission success. Continuous Risk Management (CRM) is an essential element and an integral part of NASA project management and system engineering.

Safety Program: The implementation of a formal comprehensive set of safety procedures, tasks, and activities to meet safety requirements, goals, and objectives.

Section: See “Level of Assembly.”

Single Point Failure: A single element of hardware the failure of 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.

Software Assurance: The planned and systematic set of activities that ensure that software life cycle processes and products conform to requirements, standards, and procedures. For NASA, this includes the disciplines of software quality (i.e., the functions of software quality engineering, software quality assurance, and software quality control), software safety, software reliability, software verification and validation, and IV&V.

Software Reliability: The discipline of software assurance that (1) defines the requirements for software controlled system fault/failure detection, isolation, and recovery; (2) reviews the software development processes and products for software error prevention and/or reduced functionality states; and (3) defines the process for measuring and analyzing defects and defines/derives the reliability and maintainability factors.

Software Safety: The discipline of software assurance that is a systematic approach to identifying, analyzing, tracking, mitigating and controlling software hazards and hazardous functions (data and commands) to ensure safe operation within a system.

System Safety: The application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

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 and 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 design and its ability to maintain thermal control within established mission limits for all mission phases under worst case predicted flight environments as well as provide an empirical basis to validate the thermal math model (TMM).

Thermal-Vacuum Test: A test conducted to demonstrate the capability of the test item to operate satisfactorily in vacuum at temperature levels that reflect a defined margin greater than those temperatures expected for the mission. This test will also provide a level of screening to 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 a software system or component during or at the end of the development process to determine whether it satisfies the specified requirements.

Verification: The process of evaluating a software system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. Note: for hardware verification, see “Performance Verification.”

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.

Waiver: A variance that authorizes departure from a specific requirement (including safety requirements) where a certain level of risk has been documented and accepted.

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.”)