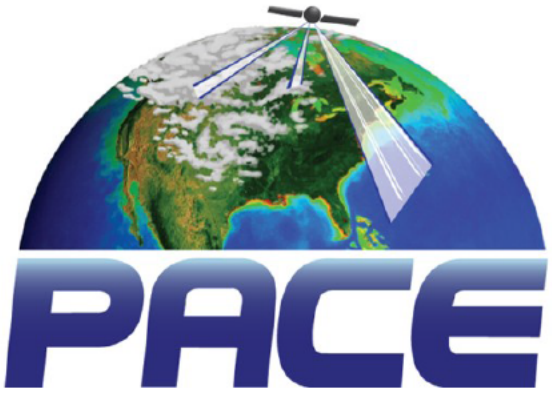
DRAFT 1

PACE-SMA-RQMT-000X, Revision -
Pre-Aerosol, Clouds, and ocean Ecosystem (PACE)

PACE Spacecraft Mission Assurance Requirements (MAR)



Goddard Space Flight Center
Greenbelt, Maryland

National Aeronautics and
Space Administration

PACE Spacecraft Mission Assurance Requirements Signature/Approval Page

Prepared by:

John C Rauscher

Reviewed by:

Approved by:

Electronic Signatures available online at: https://ipdtdms.gsfc.nasa.gov/

Preface

This document is under Pre-Aerosol, Clouds, and ocean Ecosystem (PACE) Project configuration control. Changes to this document require prior approval of the PACE Configuration Control Board (CCB) Chairperson or designee. Submit proposed changes to the PACE Configuration Management Office (CMO), along with supportive material justifying the proposed change. Changes to this document will be made by complete revision.

Change History Log

Revision	Effective Date	Description of Changes (Reference the CCR & CCB/ERB Approval Date)
-	TBD	Original Release per CCR # TBD

Table of Contents

Appendices

List of Tables

Section 1. GENERAL

1.1 Systems Safety and Mission Assurance Program

The developer shall prepare, document, and implement a Mission Assurance Implementation Plan (MAIP) in accordance with Data Item Description (DID) MA-01. The MAIP shall cover:

- Flight hardware and software that is designed, built, or provided by the developer and its subcontractors or furnished by the government, from project initiation through launch and mission operations
- The ground support equipment (GSE) that interfaces with flight items to the extent necessary to assure the integrity and safety of flight items
- The ground data system to the extent necessary to assure performance as required by the Statement of Work

Note: The developer shall request a waiver for the use of alternative processes, procedures, and standards that are proposed as alternatives to those specified by the government. The developer shall include with the waiver request a comparison matrix that identifies variances and acceptance rationales.

1.2 Management

The developer shall designate a manager for assurance activities. The assurance manager shall not be responsible for project costs and schedules other than those pertaining to assurance activities. The manager shall have direct access to management that is independent of project management and functional freedom and authority to interact with all elements of the project.

1.3 Requirements Flowdown

The developer shall apply the system safety and mission assurance requirements in this document to subcontractors and suppliers to the extent necessary to ensure that the delivered product meets performance requirements.

1.4 Suspension of Work Activities

The developer shall direct the suspension of any work activity that presents a hazard, imminent danger, or future hazard to personnel, property, or mission operations resulting from unsafe acts or conditions that are identified by inspection, test, or analysis.

1.5 Contract Data Requirements List (CDRL)

The CDRL identifies Data Item Descriptions (DID) for deliverables. The developer shall deliver data items per the requirements of the applicable DID. The developer shall perform work in accordance with the following definitions:

- Deliver for approval: The NASA GSFC Project approves the deliverable within the specified period of time before the developer proceeds with the associated work.
- Deliver for review: The NASA GSFC Project reviews the deliverable and provides comments with the specified period of time before the developer proceeds with the associated work. The developer can continue with the associated work while preparing a response to the NASA GSFC comments unless directed to stop work.
- Deliver for information: For NASA GSFC Project information only. The developer continues with the associated work.

The developer may combine deliverables if the requirements for the individual deliverables are addressed.

1.6 Surveillance

The developer shall grant access for National Aeronautics and Space Administration (NASA) and NASA assurance representatives to conduct an audit, assessment, or survey upon notice. The developer shall supply documents, records, equipment, and a work area within the developer's facilities.

Note: see Federal Acquisition Regulations (FAR) Parts 46.103, 46.104, 46.202-2, 46.4, and 46.5 for government quality assurance requirements at contractor facilities. See FAR Part 52.246 for inspection clauses by contract type.

1.7 Use of Previously Developed Product

The developer shall document the compliance of previously developed product with the system safety and mission assurance requirements (DID MA-02).

Section 2. QUALITY MANAGEMENT SYSTEM

2.1 General

The developer shall have a quality management system that is compliant with the requirements of SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing.

2.2 Supplemental Quality Management System Requirements

2.2.1 Control of Nonconforming Product

Control of Nonconforming Product – The developer shall have a documented closed loop system for identifying, reporting, and correcting product nonconformances. The system shall ensure that the adequacy of corrective action is determined by audit or test, that objective evidence is collected, and that preventive action is implemented to preclude recurrence.

2.2.2 Material Review Board (MRB)

The developer shall have a documented process for the establishment and operation of a MRB to process nonconformances, including the definitions of major and minor nonconformances. The developer shall appoint a MRB chairperson who is responsible for implementing the MRB process and functional and project representatives as MRB members. The developer shall inform the government of MRB actions (DID MA-03).

The MRB shall use the following disposition actions:

- Scrap: the product is not usable
- Re-work: the product will be re-worked to conform to requirements
- Return to supplier: the product will be returned to the supplier
- Repair: the product will be repaired using a repair process approved by the MRB
- Use as is: the product will be used as is

The developer shall request a waiver to requirements for a use-as-is disposition involving a major nonconformance (DID MA-04).

2.2.3 Anomaly Reporting and Disposition

The developer shall have a documented process for anomaly reporting and disposition. The process will establish an anomaly review board (ARB) whose membership will include a government representative as a voting member with approval authority for proposed actions.

The process will require major anomalies to be submitted to the ARB and the government (DID MA-05). The developer shall report major hardware anomalies beginning with the first application of power at the component level, major software anomalies beginning with flight software acceptance testing and when interfacing with flight hardware, and major mechanical system anomalies beginning with the first operation. Major anomalies are those that have resulted in hardware or software test failures and damage or potential damage to hardware. Examples of major anomalies are overvoltage or over current conditions, exceedance of test limits resulting in overstress, blown fuses, and unexpected system responses. The developer shall assess the failure risk ratings and failure effect risk ratings for major anomalies (see DID MA-05 for criteria) and shall identify those that have a failure effect risk rating of 2 or 3 and a failure corrective action risk rating of 3 or 4 as a significant residual risk in the risk list (see DID MA-30).

The process will allow the developer to disposition minor anomalies with an appropriate subset of the ARB. Minor anomalies are those that have caused no damage to hardware or required no change in flight software. Examples of minor anomalies are those that can be resolved immediately, procedural errors, database problems, operator errors, and exceedance of test limits that do not affect the end item.

Note: a component is defined as a functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem's operation.

Section 3. SYSTEM SAFETY

3.1 General

The developer shall document and implement a system safety program, support the Expendable Launch Vehicle (ELV) Safety Review Process as defined in paragraphs 2.4 and 2.5 of NPR 8715.7 Expendable Launch Vehicle Payload Safety Program, and meet launch services, vendor, and range safety requirements.

Specific safety requirements include the following:

- The developer shall incorporate three independent inhibits in the design (dual failure tolerant) if a system failure may lead to a catastrophic hazard. A catastrophic hazard is defined as a condition that may cause death or a permanent disabling injury or the destruction of a major system or facility on the ground or of the flight hardware during the prelaunch phase, during launch through payload separation from the launch vehicle, and during any planned recovery.
- The developer shall incorporate two independent inhibits in the design (single failure tolerant if a system failure may lead to a critical hazard. A critical hazard is defined as a condition that may cause a severe injury or occupational illness to personnel or major property damage to facilities, systems, or flight hardware.
- The developer shall adhere to specific detailed safety requirements, including compliance verification that must be met for design elements with hazards that cannot be controlled by failure tolerance. The process by which safety is incorporated into these design elements (e.g., structures and pressure vessels) is called "Design for Minimum Risk".

3.2 Mission Related Safety Requirements Documentation

The developer shall implement launch range safety requirements as applicable for the specific launch site. The most stringent applicable safety requirement shall take precedence in the event of conflicting requirements.

ELV Eastern Test Range (ETR) or Western Test Range (WTR) Missions

- NASA-STD 8719.24 (with Annex) NASA Expendable Launch Vehicle Payload Safety Requirements
- KNPR 8715.3, "KSC Safety Practices Procedural Requirements" (applicable at KSC property, KSC-controlled property, and offsite facility areas where KSC has operational responsibility)
- NPR 8715.7, "Expendable Launch Vehicle Payload Safety Program"

- Launch Site Facility-specific Safety Requirements, as applicable

3.3 System Safety Deliverables

3.3.1 System Safety Program Plan

The developer shall prepare a System Safety Program Plan (SSPP) that describes the tasks and activities of system safety management and engineering required to identify, evaluate, and eliminate or control hazards to the hardware, software, and system design by reducing the associated risk to an acceptable level throughout the system life cycle, including launch range safety requirements. (DID MA-06).

3.3.2 Safety Requirements Compliance Checklist

The developer shall document and implement a Safety Requirements Compliance Checklist to demonstrate that the payload is in compliance with NASA and range safety requirements (DID MA-07). Noncompliances to safety requirements will be documented in waivers and submitted for approval.

3.3.3 Hazard Analyses

3.3.3.1 Preliminary Hazard Analysis – The developer shall document Preliminary Hazard Analyses (PHA) (DID MA-08) to obtain an initial risk assessment and identify safety critical areas of a concept or system.

3.3.3.2 Operations Hazard Analysis (OHA) and Hazard Verification Tracking Log (VTL)

The developer shall perform and document an Operations Hazard Analysis (OHA) and a Hazard Verification Tracking Log (VTL) to demonstrate that hardware operations, test equipment operations, and integration and test (I&T) activities comply with facility safety requirements and that hazards associated with those activities are mitigated to an acceptable level of risk (DID MA-09). The developer shall update and maintain the Hazard Verification Tracking Log during I&T activities to track open issues.

3.3.3.3 Lifting Device Safety Requirements

The developer shall implement the following safety requirements for lifting devices and equipment when performing NASA work at non-NASA facilities:

- Perform and document a recognized safety hazard analysis, such as fault tree analysis, FMEA/FMECA, or Operating and Support Hazard Analysis (O&SHA), for lifting devices and equipment that will be used for critical lifts per NASA Standard 8719.9 (DID MA-10). Determination of critical lifts shall comply with the following definitions:
  - Failure/loss of control could result in loss of or damage to flight hardware, a lift involving special high dollar items such as spacecraft, one-of-a-kind articles, or major facility components, whose loss would have serious programmatic or institutional impact.
  - The lifting of personnel with a crane.
  - Where personnel are required to work under a suspended load
  - Operations with special personnel and equipment safety concerns beyond normal lifting hazards.
- Ensure that for critical lifts overhead cranes, winches, and hoists have dual holding brakes and dual upper limit switches installed as defined in NASA Standard 8719.9 paragraphs 4.2.6 and 4.2.7;
- Ensure that for non-critical lifts cranes comply with applicable ANSI/ASME B30 and B56 standards.
- Ensure that medical examinations for crane operators comply with the requirements of applicable ANSI/ASME lifting device standards (e.g., B30, B56).
- Ensure that a NCCCO (National Commission for the Certification of Crane Operators) certified or equivalent trainer train lifting device and equipment operators and riggers.
- Use qualified employees or contractors for training programs and maintain relevant documentation.

- Perform periodic load testing in accordance with NASA-STD-8719.9 (paragraphs 4.3, 5.3, 7.3, 8.3 and 10.3) for the following lifting devices and equipment: overhead cranes; mobile cranes and derricks; hooks hydra-sets and load measuring devices; and slings and riggings.
- Perform the load testing for overhead cranes used for critical lifts at a minimum of four-year intervals.
- Perform daily and formal periodic inspections the following lifting devices and equipment: overhead cranes; mobile cranes and derricks; hooks hydra-sets and load measuring devices; and slings and riggings in accordance with NASA-STD-8719.9 (paragraphs 4.4, 5.4, 7.4, 8.4 and 10.4).
- Perform nondestructive testing (NDT) inspections using an American Society of Nondestructive Testing (ASNT) or equivalently trained inspector on critical lifting hardware and equipment after initial proof test and load testing.
- Label and tag lifting devices and equipment per NASA-STD-8719.9 (paragraphs 4.2.2, 5.2.2, 8.2.2 and 10.2.2).
- Ensure that personnel shall not be under suspended or moving loads unless the operation adheres to the OSHA-approved NASA Alternate Standard for Suspended Load Operations (see Appendix A of NASA-STD-8719.9).
- Ensure that lifting of personnel with a crane shall be in accordance with 29 CFR 1926.550 (see Appendix C of NASA-STD-8719.9.

3.3.3.4 Operating and Support Hazard Analysis – The developer shall perform and document an Operating and Support Hazard Analyses (O&SHA) to evaluate activities for hazards introduced during pre-launch processing and to evaluate the adequacy of operational and support procedures used to eliminate, control, or mitigate hazards (DID MA-11).

3.3.4 Safety Data Package (SDP)

The developer shall prepare an integrated SDP to document the results of hazard analyses identifying the prelaunch, launch and ascent hazards associated with the flight system, ground support equipment, and their interfaces in hazard reports (DID MA-12).

3.3.5 Verification Tracking Log (VTL)

The developer shall prepare, implement, and maintain a SDP VTL (DID MA-13).

3.3.6 Hazardous Procedures for I&T and Pre-launch Processing

The developer shall document and implement hazardous procedures that comply with applicable facility safety requirements when performing integration and test activities and pre-launch activities at the launch site (DID MA-14). The developer shall provide safety support for hazardous operations at the launch site.

3.3.7 Safety Waivers

The developer shall request waivers for variations from the applicable safety requirements per paragraph 1.5 of NPR 8715.7 (DID MA-15).

3.3.8 Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)

The developer shall provide the inputs necessary for the development of the ODAR and the EOMP per the content defined in NASA-STD 8719.14, (DID MA-16).

3.3.9 Mishap Reporting and Investigation

The developer shall prepare a Pre-Mishap Plan that describes appropriate mishap and close call notification, reporting, recording, and investigation procedures (DID MA-17). The developer shall report accidents, test failures, or other mishaps and close calls promptly to NASA. The developer shall promptly investigate so as to determine the root cause.

3.3.10 Range Safety Forms

The developer shall prepare the following forms (DID MA-18):

- KTI-5212 Material Selection List for Plastic Films, Foams, and Adhesive Tapes
- KSC FORM 16-294 NS Radiation Training and Experience Summary (Ionizing Radiation)
- KSC FORM 16-295 NS Radiation Use Request/Authorization (Radiation Materials)
- KSC FORM 16-447 Laser Device Use Request/Authorization
- KSC FORM 16-450 NS Radiation Training & Experience Summary (Non-ionizing Radiation)
- KSC FORM 16-451 NS Radio Frequency/Microwave System Use Request/ Authorization
- KSC Form 26-551V2 Process Waste Questionnaire
- AF Form 813 Request for Environmental Impact Analysis

Section 4. PROBABILISTIC RISK ASSESSMENT (PRA) AND RELIABILITY

4.1 Reliability Program Plan (RPP)

The developer shall document and implement a Reliability Program Plan, including the developer's approach to PRA requirements in section 4.2, using both qualitative and quantitative techniques to support decisions regarding mission success and safety throughout system development (DID MA-19). The RPP shall include a detailed approach to the analysis of hardware and software for their contributions to system reliability and mission success.

4.2 Probabilistic Risk Assessment (PRA)

The developer shall perform a PRA per NPR 8705.5, Probabilistic Risk Assessment (PRA) Technical Procedures for Safety and Mission Success for NASA Programs and Projects (DID MA-20).

4.3 FMEA/FMECA and Critical Items List (CIL)

The developer shall perform an FMEA/FMECA (Failure Modes and Effects/Failure Modes and Effects Criticality Analysis) to identify potential failures with severity categories 1, 1R, 1S, 2, 2R, 3, and 4 per Table 4.1 (DID MA-21).

The developer shall prepare and maintain a CIL for severity categories 1, 1R, 1S, and 2 per Table 4.1 (DID MA-21).

The developer shall:

- Analyze failure modes resulting in severity categories 1, 1R, 1S, or 2 to determine the potential cause, corresponding mitigation actions, and retention rationale.
- Identify and assess common cause failure modes and causes for category 1R items
- Address flight hardware and software that is designed, built, or provided by their organization or subcontractors, from project initiation through launch and mission operations.
- Address the ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items.
- Identify and address safety critical software, as defined in Sction 5.

Table 4.1 Severity Categories

Category	Description
1	Catastrophic failure modes that may cause death or a permanent disabling injury or the destruction of a major system or facility on the ground or of the vehicle during the mission. Critical failure modes that could in a condition that may cause a severe injury or occupational illness to personnel or major property damage to facilities, systems, or flight hardware.
1R	Failure modes of identical or equivalent redundant hardware or software elements that could result in Category 1 effects if all failed.
1S	Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.
2	Failure modes that could result in loss of one or more mission objectives as defined by the NASA GSFC project office.
2R	Failure modes of identical or equivalent redundant hardware or software that could result in Category 2 effects if all failed.
3	Failure modes that could cause degradation to mission objectives.
4	Failure modes that could result in insignificant or no loss to mission objectives

4.4 Fault Tree Analysis

The developer shall perform qualitative fault tree analyses to address mission failures and degraded modes of operation (DID MA-22). The fault tree analyses shall be extended to include software contributions to loss of mission scenarios. The developer shall perform quantitative fault tree analysis to address undesirable fault propagation scenarios/events as part of the PRA.

4.5 Parts Stress Analysis

The developer shall perform parts stress and derating analyses for electrical, electronic, and electromechanical (EEE) parts in accordance with GSFC INST-EEE-002 Instruction for EEE Parts Selection, Screening, Qualification, and Derating (DID MA-23).

4.6 Worst-Case Analysis

The developer shall perform worst-case analyses (WCA) for circuits (DID MA-24)

4.7 Reliability Assessments and Predictions

The developer shall perform comparative numerical reliability assessments and reliability predictions (DID MA-25).

4.8 Trend Analysis

The developer shall prepare and maintain a list of subsystem and components to be assessed, parameters to be monitored, and trend analysis reports as defined in the approved PRA and Reliability Program Plan. The developer shall begin the monitoring, collection, and analysis at component acceptance testing and continue through the system integration and test phases.

4.9 Analysis of Test Results

The developer shall document the analysis of test information, trend data, and failure investigations to assess reliability and identify potential or existing problem areas. The developer shall report the results as defined in the approved Reliablity Program Plan.

4.10 Limited Life Items

The developer shall prepare and implement a plan to identify and manage limited life items (DID MA-26).

Section 5. SOFTWARE ASSURANCE

5.1 Applicable Software Definitions

When identifying, developing, verifying, and maintaining software, the developer shall apply the following definitions:

> Software is defined as computer programs, procedures, scripts, rules, and associated documentation and data pertaining to the development and operation of a computer system. Software includes commercial–off-the-shelf (COTS) software, government-off-the-shelf (GOTS) software, modified-off-the-shelf (MOTS) software, custom software, reused software, heritage software, auto generated code, and code executed on microprocessors.
>
> Mission-Critical Software - Software that can cause, contribute to, or mitigate the loss of capabilities that are essential to the primary mission objectives. The software reliability assessment and analysis is focused on failure modes specific to post-separation mission phases.
>
> Safety-Critical Software - Software that can cause, contribute to, or mitigate human safety hazards or damage to flight hardware and facilities. The software safety assessment and analysis is focused on hazards specific to Integration and Test, launch, and up through spacecraft separation from the launch vehicle (except for International Space Station (ISS) payloads that have constant human presence) and re-entry/recovery (where applicable).

Note: The above definitions for Mission and Safety Critical Software are derived from Safety Critical as defined by the NASA Software Standard. The delineation is meant only to provide clarification for organizations with separate processes for assessing pre-separation and post-separation hazards and failures. Both categories of software must comply with the NASA-STD-8719.13 Software Safety Standard, which requires assessment of the entire lifecycle for potential injury, major damage, or mission failure.

5.2 Software Assurance Program

The developer shall plan and implement a Software Assurance Program that complies with the definitions in 5.1 and:

- NASA-STD-8739.8 NASA Standard for Software Assurance
- NASA-STD-8719.13 Software Safety Standard

The developer shall identify the person responsible for directing and managing the software assurance program and interfacing with government assurance personnel.

The developer shall document the software assurance program in a Software Assurance Plan (DID MA-27). The plan will address the disciplines of Software Quality, Software Safety, Software Reliability, Software Verification and Validation (V&V), and Independent Verification and Validation (IV&V) and detail the role of assurance and their activities in ensuring quality products and processes for each discipline. The plan will include the software assurance processes, procedures, tools, and techniques to be used commensurate with the Software Classification Assessment. The plan will address software assurance the necessary collaboration between software assurance, system safety, system reliability, and software engineering.

5.2.1 Software Quality

The developer shall evaluate software processes and work products as defined by NPR 7150.2 and commensurate with the software classification. The developer shall identify and document noncompliance issues, communicate the results of quality assurance activities, maintain records, and ensure disposition of noncompliances.

5.2.2 Software Safety Analysis

The developer shall identify safety critical software per Appendix A of NASA-STD-8719.13 Software Safety Standard. For software that is safety critical, the developer shall perform Software Safety Analyses per NASA-STD-8719.13 Standard for Software Safety to a) identify whether software can contribute to a hazard (for example, as a cause or control), b) identify specific software modules or functions associated with the hazard cause, c) identify hazard elimination and hazard control methodologies and associated software safety requirements, and d) verify that the inhibits and controls incorporated to eliminate or mitigate hazards are effective.

The developer shall incorporate the results from the Software Safety Analyses, including references to the associated software requirements, into hazard reports and deliver as part of the SDP (DID MA-12).

5.2.3 Software Reliability Analysis

The developer shall include in the software plan processes and procedures to identify mission critical software and to design robust performance and fault tolerance into such components. The developer shall include details regarding the following:

- Integration of software into system-level and component reliability analysis, and identifying software components critical to the success of nominal operations
- Derivation and flowdown of software fault and failure management requirements from system-level and component reliability analysis
- Identification of mission critical software requirements and performance specifications
- Traceability and consistency between reliability analysis and the software design
- Provisions for high-fidelity validation of mission critical software

5.2.4 Verification and Validation

The developer shall review the software section of the Verification and Validation Plan/Test Plan and review and support walkthroughs of test procedures. The developer shall witness or review results of software testing, review software discrepancy reports, and review software delivery documentation. The developer shall document software discrepancy reports and participate in failure review boards to resolve outstanding software-related issues.

5.2.5 Independent Verification and Validation

The developer shall provide required information (i.e., access to software products and processes) to IV&V personnel and address corrective actions.

5.3 Reviews

In addition to the reviews specified in Section 8 and NPR 7150.2 (Section 4.3), the developer shall conduct the following:

- Software test readiness reviews
- Software acceptance reviews
- System level safety reviews

The developer shall provide advance notification, as well as the review materials, prior to all reviews.

5.4 Surveillance of Software Development, Maintenance, and Assurance Activities

The developer shall provide the following:

- Direct access to the software problem reporting system
- Electronic access to the software documentation (i.e., management plans, assurance plans, configuration management plans, requirements specifications, design documents, test plans, test cases, test procedures, test results, schedule, maintenance plans)
- Electronic access to the software review results
- Electronic access to source code
- Schedule of software development activities and critical milestones
- Schedule of assurance reviews, audits, and assessments of the developer's processes and products
- Access to the corrective actions from process and product audits
- Access to review action item status and resolution
- Access to monthly software measurement and metrics data prepared per the requirements of NPR 7150.2 NASA Software Engineering Requirements
- Access to requirements traceability matrices and data prepared per the requirements of NPR 7150.2 NASA Software Engineering Requirements
- Software Assurance Status Report (DID MA-28)

Section 6. DIGITAL ELECTRONIC COMPONENTS

6.1 General

The developer shall document and implement an assurance plan for covered digital electronic components and designs as specified below. The plan will address: parts selection; version control; timing verification; routing analysis verification; monitoring, witnessing, and inspection points; system safety, including analyses of irreversible processes; reliability; peer reviews. A FPGA or ASIC development plan with the same content will be sufficient to meet this requirement.

Covered digital electronic components are:

- Gate array technologies, including mask programmed gate arrays, field programmable gate arrays, custom ASICs, and the digital sections of mixed-signal ASICs
- And-Or plane devices, such as PALs and PLAs

The plan does not apply to software or firmware executed on processors or memory devices; this is subject to the relevant requirements of software assurance in Section 5.

The developer shall identify the person responsible for directing and managing the digital electronic components assurance program and interfacing with government assurance personnel.

6.2 Peer Reviews

The developer shall conduct peer reviews that encompass the following:

- Design (place and route) database and any constraint file(s)
- Synthesis report files
- Timing analyses for external inputs and outputs, internal domain(s), etc.
- Disposition of all clock domain crossings
- Source code (eg VHDL or Verilog), PDF of schematics and/or state machines/tables
- Requirements, specifications, and verification document(s), and any supporting material (e.g. block diagrams, presentation material) relevant to the FPGA
- Simulation code coverage analysis and simulation testbench/script code

- Source code for 3rd party intellectual property code and/or cores
- FPGA Design Checklist as per 500-PG-8700-2.7, or equivalent
- Board(s) schematics containing this FPGA
- Board netlist(s) (any ASCII format such as PADS, MGC, Allegro)

The following items are desirable but not required for peer reviews:

- System, box, and circuit board requirements, specifications, presentations, and/or verification document(s) relevant to the FPGA and its role in the system, box, and board
- Board(s) schematics containing this FPGA
- Board netlist(s) (any ASCII format such as PADS, MGC, Allegro)
- Board part list (any ASCII or common spreadsheet format)
- PDF of the board layout, such as an assembly drawing
- Signal integrity analyses relevant to this FPGA
- Power integrity analyses relevant to this FPGA

Section 7. RISK MANAGEMENT

7.1 General

The developer shall document and implement a risk management plan (DID MA-29).

7.2 Risk List

The developer shall prepare and maintain a risk list (DID MA-30).

Section 8. SYSTEMS REVIEWS

8.1 Systems Reviews

The developer shall participate in the implementation of the Systems Review Program (SRP) as required by GSFC-STD-1001 Criteria for Flight and Flight Support Systems Lifecycle Reviews.

The developer shall provide a review agenda, presentation materials, and a copy of reference materials at the reviews (DID MA-31).

The developer shall submit responses to review action items (DID MA-32).

8.2 Peer Reviews

The developer shall prepare and implement an engineering peer review program that covers the design, development, and testing of hardware and software (DID MA-33).

Section 9. SYSTEM PERFORMANCE VERIFICATION

9.1 System Performance Verification Program Plan

The developer shall plan and implement a system performance verification program per the requirements of GSFC-STD-7000 General Environmental Verification Standard (DID MA-34).

9.2 Integration, Test, and Verification Plan

The developer shall prepare and implement an integration, test, and verification plan that includes the environmental verification plan (DID MA-35).

9.3 System Performance Verification Matrix

The developer shall prepare and maintain a system performance verification matrix (DID MA-36).

9.4 Integration, Test, and Verification Matrix

The developer shall prepare and maintain an environmental test matrix (DID MA-37).

9.5 Verification Reports

The developer shall prepare and submit verification reports, including system performance reports (DID MA-38).

Section 10. WORKMANSHIP

10.1 General

The developer shall implement a workmanship program to assure that electronic packaging technologies, processes, and workmanship meet mission objectives for quality and reliability per the requirements of the following standards:

- NASA-STD-8739.1 Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
- NASA-STD-8739.4 Crimping, Interconnecting Cables, Harnesses, and Wiring
- NASA-STD-8739.5 Fiber Optic Terminations, Cable Assemblies, and Installation
- NASA-STD-8739.6, Implementation Requirements for NASA Workmanship Standards
- GSFC-STD-6001, Ceramic Column Grid Array Design and Manufacturing Rules for Flight Hardware
- IPC-J-STD-001ES, Joint Industry Standard, Space Applications Electronic Hardware Addendum (except Chapter 10 of IPC-J-STD-001E)
- IPC-2221 Generic Standard on Printed Board Design (except paragraph 3.1.1)
- IPC-2222 Sectional Design Standard for Rigid Organic Printed Boards
- IPC-2223 Sectional Design Standard for Flexible Printed Boards
- IPC-2225 Sectional Design Standard for Organic Multichip Modules (MCM-L) and MCM-L Assemblies
- IPC A-600 Acceptability of Printed Boards (Class 3 requirements)
- IPC-6011 Generic Performance Specification for Printed Boards (Class 3 requirements; except paragraph 3.5)
- IPC-6012 Qualification and Performance Specification for Rigid Printed Boards (Class 3/A requirements)
- IPC-6013 Qualification and Performance Specification for Flexible Printed Boards (Class 3 requirements)
- IPC-6015 Qualification and Performance Specification for Organic Multichip Module (MCM-L) Mounting and Interconnecting Structures
- IPC-6018 Microwave End Product Board Inspection and Test (Class 3 requirements)

10.2 Design and Process Qualification

The developer shall perform and document qualification of designs and processes that are not covered by or do not conform to the above standards

10.3 Electrostatic Discharge Control (ESD)

The developer shall prepare and implement an ESD control program that conforms to the requirements of ANSI/ESD S20.20, Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices) (DID MA-39).

10.4 Splices, Circuit Board Trace Cuts, and Jumper Wires

The developer shall not incorporate splices, board trace cuts, or jumper wires that result from repairs or design changes into flight hardware, including previously developed hardware, until approved by the MRB.

Section 11. EEE PARTS

11.1 General

The developer shall document and implement a parts control plan (PCP) per the Level 3 requirements of NASA GSFC EEE-INST-002 Instruction for EEE Parts Selection, Screening, Qualification, and Derating (DID MA-40) and Level 2 requirements (per EEE-INST-002) shall apply for applications that represent potential single point failures. Destructive Parts Analysis (DPA) shall be completed for hybrid parts, and pre-cap inspection shall be performed on hybrid parts with Government participation.

The developer shall identify the person responsible for directing and managing the EEE parts program and interfacing with government assurance personnel.

11.2 Parts Control Board

The developer shall establish a parts control board (PCB) that is responsible for the planning, management, and coordination of the selection, application, and procurement requirements of EEE parts (DID MA-41). The government Parts Engineer shall be included as a voting member of the PCB.

11.3 Re-use of EEE Parts

The developer shall require approval of the MRB to re-use EEE parts that have been installed and removed other than as planned and designed.

11.4 EEE Parts Lists

The developer shall develop and maintain EEE parts lists.

11.4.1 Parts Identification List (PIL)

The developer shall prepare a list of EEE parts that are proposed for use in flight hardware and approved by the PCB (DID MA-42).

11.4.2 Project Approved Parts List (PAPL)

The developer shall prepare a list of EEE parts that are approved for use in flight hardware by the PCB (DID MA-43).

11.4.3 As-designed Parts List (ADPL)

The developer shall prepare a list of EEE parts that are used in the design of flight hardware (DID MA-44).

11.4.4 As-built Parts List (ABPL)

The developer shall prepare a list of EEE parts that are used in the flight hardware (DID MA-45).

Section 12. MATERIALS AND PROCESSES

12.1 General

The developer shall prepare and implement a materials and processes selection, control, and implementation plan (DID MA-46).

12.2 Life Test Plan for Lubricated Mechanisms

The developer shall prepare and implement a life test plan for lubricated mechanisms (DID MA-47).

12.3 Materials Usage Agreement (MUA)

The developer shall prepare materials usage agreements (DID MA-48).

12.4 Materials Identification and Usage List (MIUL)

The developer shall prepare a materials identification and usage list (DID MA-49).

Note: Soldering flux shall be included in the MIUL. Solvents used for cleaning flight electronic assemblies other than isopropyl alcohol or deionized water shall be included in the MIUL.

12.5 Nondestructive Evaluation (NDE) Plan

The developer shall prepare and implement a nondestructive evaluation plan for the procedures and specifications used in the inspection of materials (DID MA-50).

12.6 Printed Wiring Board (PWB) Test Coupons

The developer shall provide printed wiring board test coupons to NASA GSFC or to a NASA GSFC-approved facility for analysis (DID MA-51).

The developer shall not use printed wiring boards until coupon analysis results are received.

12.7 Titanium Alloys

The developer shall use the specifications superseding SAE AMS-T-9046 and SAE AMS-T-9047 to procure titanium.

The developer shall reduce design allowables to 110 ksi yield and 120 ksi ultimate for all Ti-6Al-4V hardware produced from billet and reduce other properties, such as shear and compression strength, by ten percent (10%). The developer shall have billet properties independently verified if reduced allowables are insufficient to provide adequate safety margins and shall document the properties in a Materials Usage Agreement (MUA).

Products that cannot be manufactured from a billet, such as sheet, rod, tubing, extruded stock, and fasteners, do not require additional testing.

Section 13. CONTAMINATION CONTROL

13.1 Contamination Control Plan

The developer shall prepare and implement a contamination control program (DID MA-52).

13.2 Foreign Object Debris Program

The developer shall prepare and implement a foreign object debris program (DID MA-53).

Section 14. METROLOGY AND CALIBRATION

14.1 Metrology and Calibration Program

The developer shall comply with one of the following standards for the calibration of measuring and test equipment:

- ANSI/NCSL Z540.1-1994 (R2002) Calibration Laboratories & Measuring & Test Equipment - General Requirements
- ANSI/NCSL Z540.3-2006 Requirements for the Calibration of Measuring and Test Equipment
- ISO 17025-2002 General requirements for the competence of testing and calibration laboratories

14.2 Use of Calibrated and Non-calibrated Instruments

The developer shall maintain the calibration of test and measuring equipment and safety instruments used for: acceptance testing; inspection; maintenance; flight hardware qualification; measurement where accuracy is essential for the safety of personnel or the public; telecommunication, transmission, and test equipment where exact signal interfaces and circuit confirmations are essential to mission success; development, testing, and special applications where the specifications, end products, or data are accuracy sensitive, including instruments used in hazardous and critical applications

The developer shall limit the use of non-calibrated instruments to applications where substantiated accuracy is not required and for indication-only purposes in non-hazardous, non-critical applications.

Section 15. GIDEP ALERTS AND PROBLEM ADVISORIES

15.1 Government-Industry Data Exchange Program (GIDEP)

The developer shall participate in GIDEP per the GIDEP Operations Manual S0300-BT-PRO-010 and GIDEP Requirements Guide S0300-BU-GYD-010 (Note: these documents are available through http://www.gidep.org).

15.2 Alert Disposition

The developer shall review the following, hereafter referred to collectively as Alerts, for affects on EEE parts, materials, equipment and software used in NASA products: GIDEP Alerts; GIDEP SAFE-ALERTS; GIDEP Problem Advisories; GIDEP Agency Action Notices; NASA Advisories.

The developer shall eliminate or mitigate the effects of Alerts on NASA products.

The developer shall report the disposition of Alerts (DID MA-54).

15.3 GIDEP Reporting

The developer shall prepare and submit failure experience data and safety issue reports per the requirements of S0300-BT-PRO-010 and S0300-BU-GYD-010 whenever failed or nonconforming items that are available to other buyers are discovered (DID MA-55).

15.4 Review Reporting

The developer shall report the status of NASA products that are affected by Alerts or by significant EEE parts, materials, and safety problems at program milestone reviews and readiness reviews (see Section 8). The developer shall include a summary of the review status for EEE parts and materials lists and of actions taken to eliminate or mitigate negative effects.

Section 16. END ITEM ACCEPTANCE DATA PACKAGE

The developer shall submit an end item acceptance data package (DID MA-56).

Appendix A. Acronym List

ABPL	As-built Parts List
ADPL	As-designed Parts List
ARB	Anomaly Review Board
ANSI	American National Standards Institute
ASIC	Application Specific Integrated Circuit
ASME	American Society of Mechanical Engineers
ASNT	American Society for Nondestructive Testing
CAF	Conductive Anodic Filament
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFR	Code of Federal Regulations
CIL	Critical Items List
CIT	Certified IPC Trainer
CMMI	Capability Maturity Model Integration
COTS	Commercial off-the-shelf software
CR	Change Request
CSCIs –	Computer software configuration items
DID	Data Item Description
DR	Discrepancy Report
EEE	Electrical, Electronic, and Electromechanical
ELV	Expendable Launch Vehicle
EOMP	End of Mission Plan
ESD	Electrostatic Discharge Control
FAR	Federal Acquisition Requirements
FBD	Function Block Diagram
FMEA/FMECA	Failure Modes and Effects Analysis/Failure Modes and Effects Criticality Analysis
FSC	Federal Supplier Code
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GIDEP	Government-Industry Data Exchange Program
GOTS	Government off-the-shelf software
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
I&T	Integration and Test
IIRP	Integrated Independent Review Program
ISAR	Instrument Safety Assessment Report
IV&V	Independent Verification and Validation
LFCP	Lead-Free Control Plan
M&P	Materials and Processes
MAIP	Mission Assurance Implementation Plan
MAPTIS	Materials and Processes Technical Information System
MOTS	Modified off-the-shelf software
MRB	Material Review Board
MUA	Materials Usage Agreement
MIUL	Materials Identification and Usage List
NASA	National Aeronautics and Space Administration
NCCCO	National Commission for the Certification of Crane Operators
NDE	Nondestructive Evaluation
NPR	NASA Procedural Requirement
O&SHA	Operating and Support Hazard Analyses
ODAR	Orbital Debris Assessment Report
OHA	Operations Hazard Analysis
PAL	Programmable Array Logic

PAPL	Project Approved Parts List
PCB	Parts control board
PCP	Parts Control Plan
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analyses
PIL	Parts Identification List
PLA	Programmable Logic Array
PPQA	Process and Product Quality Assurance
PRA	Probabilistic Risk Assessment
PSR	Pre-Ship Review
PWB	Printed Wiring Board
RPP	Reliability Program Plan
SAE	Society of Automotive Engineers
SCM	Software Configuration Management
SDP	Safety Data Package – STS missions only
SMA	Safety and Mission Assurance
SMA-D	Safety and Mission Assurance Directorate
SOW	Statement of Work
SQAP	Software Quality Assurance Plan
SRP	Systems Review Program
SSPP	System Safety Program Plan
V&V	Verification and Validation
VDD	Version Description Documents
VTL	Verification Tracking Log
WCA	Worst Case Analysis

Appendix B. Data Item Descriptions

DID MA-01 MISSION ASSURANCE IMPLEMENTATION PLAN

Title: Mission Assurance Implementation Plan	DID No.: MA-01
MAR Paragraph: 1.1	
Use: Documents the developer's plan for implementing a system safety and mission assurance program.	
Reference Documents:	
Place/Time/Purpose of Delivery: • Deliver plan to the Project Office sixty (60) days after contract award for information • Deliver updates to the plan to the Project Office thirty (30) days prior to implementation for information	
Preparation Information: The MAIP shall cover: • All flight hardware and software that is designed, built, or provided by the developer and its subcontractors, or furnished by the government, from project initiation through launch and mission operations • Ground Support Equipment (GSE) that interfaces with flight equipment • The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items • The ground data system The MAIP shall include a traceability matrix for the mission assurance requirements	

DID MA-02 PREVIOUSLY DEVELOPED PRODUCT – COMPLIANCE WITH REQUIREMENTS

Title: Previously Developed Product – Compliance with Requirements	DID No.: MA-02
MAR Paragraph: 1.7	
Use: Documents the compliance of previously developed product with the system safety and mission assurance requirements of the MAR.	
Reference Documents: • MAR	
Place/Time/Purpose of Delivery: • Deliver to the Project Office thirty 30 days after identification of the previously developed product for approval.	
Preparation Information: The document shall identify the system safety and mission assurance requirements that apply to the previously developed product through a requirements compliance matrix for the product's specific characteristics and its development. The document shall address all areas of noncompliance through the submission of waiver requests to the relevant requirements.	

DID MA-03 REPORTING OF MRB ACTIONS

Title: Reporting of MRB Actions	DID No.: MA-03
MAR Paragraph: 2.2.2	
Use: Report MRB actions to the project office.	
Reference Documents: • SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing	
Place/Time/Purpose of Delivery: • Major MRB actions: Deliver to the project office within five (5) working days of MRB action for approval. • Minor MRB actions: Deliver to the project office within five (5) working days of MRB action for review.	
Preparation Information: • The developer shall document document relevant information on a developer MRB form that includes at least the following: o The developer shall document relevant information on a developer MRB form that includes at least the following: o Identification of project, system, or sub-system o Identification of item (e.g., assembly, sub-assembly, or part, to include serial number or part number as applicable) o Description of affected item o Definition of major and minor nonconformances o Identification of next higher assembly o Description of anomaly, including activities leading up to the anomaly o Names and contact information of involved individuals o Status of item o Contact information for personnel who originated the report o Date of original submission to the MRB o Actions taken after approval	

DID MA-04 REQUEST FOR A WAIVER

Title: Request for a waiver	DID No.: MA-04
MAR Paragraph: 2.2.2	
Use: Request government approval of a waiver.	
Reference Documents: • SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing	
Place/Time/Purpose of Delivery: • Deliver to the Project Office within five (5) working days of identifying the need for a waiver for approval.	
Preparation Information: The developer shall identify the requirements that apply to the product and provide specific information regarding the noncompliance of the product with the requirements. The developer shall identify the effect of the proposed noncompliance on product performance at higher levels of assembly.	

DID MA-05 MAJOR ANOMALY REPORT

Title: Major Anomaly Report	DID No.: MA-05

MAR Paragraph: 2.2.3

Use:

Document anomalies, investigative activities, rationale for closure, and corrective and preventive actions.

Reference Documents:

- SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing

Place/Time/Purpose of Delivery:

- Deliver initial submission to the project office within 24 hours of occurrence for information.
- Deliver notice of a change in status within 24 hours of occurrence for information.
- Deliver the proposed closure to the project office prior to closure for approval.

Preparation Information:

Document anomalies, changes in status, or proposed closure to identify the following information:

- Identification of project, system, or sub-system
- Identification of failed item (e.g., assembly, sub-assembly, or part)
- Description of item
- Identification of next higher assembly
- Description of anomaly, including activities leading up to anomaly, if known
- Names and contact information of individuals involved in anomaly
- Date and time of anomaly
- Status of item
- Contact information for personnel who originated the report
- Date of original submission
- Anomaly cause
- Corrective actions implemented
- Retesting performed and results
- Other items affected
- Risk ratings – the numerical ratings for failure effect risk and corrective action risk per the following criteria:
  a. Failure Effect Risk Rating – indicates the potential impact of the anomaly on hardware or software performance if it occurred during the mission. Redundancy shall be ignored in establishing this rating. The project shall assign a failure effect risk rating per the following criteria: and corresponding numerical values:
     1. Negligible or no effect on mission, system or instrument performance, reliability or safety.
     2. Moderate or significant effect on the mission, system or instrument performance, reliability or safety, defined as: an appreciable change in functional capability, an appreciable degradation of engineering or science telemetry, causing significant operational difficulties or constraints, or causing a reduction in mission lifetime.
     3. Catastrophic or major degradation to mission, system or instrument performance, reliability or safety.
  b. Corrective Action Rating – indicates the confidence in the root cause and the corrective action. The project shall assign a failure corrective action risk rating per the following criteria:
     1. Recurrence very unlikely – the root cause of the anomaly has been determined with confidence by analysis or test. Corrective action has been determined, implemented, and verified with certainty. There is a very low probability of recurrence.
     2. Recurrence unlikely – the root cause of the anomaly has not been determined with confidence.

However, some corrective action has been determined, implemented, and verified to the extent that there is a very low probability of recurrence.

3. Recurrence possible – the root cause is considered known and understood with confidence. Corrective action has not been determined, implemented, or verified with certainty. There exists a possibility that the anomaly may recur.
4. Recurrence credible – the root cause has not been determined with confidence. Corrective action has not been determined, implemented, or verified with certainty. There exists a possibility that the anomaly may recur.

DID MA-06 SYSTEM SAFETY PROGRAM PLAN

Title: System Safety Program Plan	DID No.: MA-06
MAR Paragraph: 3.3.1	

Use:

The System Safety Program Plan (SSPP) describes the tasks and activities of system safety management and engineering required to identify, evaluate, and eliminate or control hazards to the hardware, software, and system design by reducing the associated risk to an acceptable level throughout the system life cycle.

Reference Documents:

- NPR 8715.7 Expendable Launch Vehicle Payload Safety Program
- NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements

Place/Time/Purpose of Delivery:

- Deliver preliminary plan to the Project Office at SRR for information.
- Deliver final plan to the Project Office forty-five (45) days prior to PDR for information.
- Deliver updates to the final plan to the Project Office thirty (30) days prior to implementation for information

Preparation Information:

The developer shall prepare a SSPP that describes the development and implementation of a system safety program that complies with the requirements of NPR 8715.7, the launch service provider, and launch range safety. The developer shall

- Define the roles and responsibilities of personnel
- Define the required documentation, applicable requirements documents, and completion schedules for analyses, reviews, and safety packages
- Address support for Safety Reviews, Safety Working Group Meetings and TIMs
- Provide for early identification and control of hazards to personnel, facilities, support equipment, and the flight system during product development, including design, fabrication, test, transportation, and ground activities.
- Address compliance with the launch range safety requirements
- Include a safety review process that meets the requirements of NASA-STD-8715.7 Expendable Launch Vehicle Payloads Safety Program
- Address compliance with industrial safety requirements imposed by NASA and OSHA design and operational needs (e.g., NASA-STD-8719.9 Lifting Devices and Equipment as applicable) and contractually imposed mission unique obligations

DID MA-07 SAFETY REQUIREMENTS COMPLIANCE CHECKLIST

Title: Safety Requirements Compliance Checklist	DID No.: MA-07
MAR Paragraph: 3.3.2	

Use:

The checklist indicates for each requirement whether the proposed design is compliant, non-compliant but meets intent, non-compliant, or if the requirement is not applicable. An indication other than compliant will include rationale.

Note: the developer shall submit safety waivers for non-compliant design elements per paragraph 3.2.7 and DID MA-15.

Reference Documents:

- NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements
- Reference MAR Section 3.1.1, Mission Related Safety Requirements Documentation

Place/Time/Purpose of Delivery:

- Deliver preliminary version to the Project Office forty-five (45) days prior to PDR for approval.
- Deliver final version to the Project Office forty-five (45) days prior to CDR for approval.

Preparation Information:

The developer shall prepare a compliance checklist of all design, test, analysis, and data submittal requirements. The following shall be included:

- Criteria and requirement.
- System
- Indication of compliance, noncompliance, or not applicable
- Rationale for indications other than compliant
- Resolution
- Reference
- Copies of Range Safety and NASA approved non-compliances, including waivers and equivalent levels of safety certifications

DID MA-08 PRELIMINARY HAZARD ANALYSIS

Title: Preliminary Hazard Analysis	DID No.: MA-08

MAR Paragraph: 3.3.3.1

Use:

The Preliminary Hazard Analysis (PHA) is used to obtain an initial risk assessment and identify safety critical areas of a concept or system. It is based on the best available data, including mishap data from similar systems and other lessons learned. The developer shall evaluate hazards associated with the proposed design or function for severity, control approach (fault tolerance or design for minimum risk), and operational constraints. The developer shall identify safety provisions and alternatives that are needed to eliminate hazards or reduce their associated risk to an acceptable level.

Reference Documents:

- NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements
- JMR 002, Launch Vehicle Payload Safety Requirements
- NPR 8715.7, ELV Payload Safety Program
- MIL-STD-882E, Standard Practice for System Safety, Appendix B

Place/Time/Purpose of Delivery:

- Submit the PHA with the SDP I (DID MA-12) to the Project Office for approval.

Preparation Information:

The PHA shall consider the following for identification and evaluation of hazards as a minimum:

- Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).
- Safety related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This shall include consideration of the potential contribution by software (including software developed by other contractors/sources) to subsystem/system mishaps that occur prior to separation from launch vehicle on-orbit. Safety design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or other undesired events) shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.
- Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation).
- Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures. Those test unique hazards which will be a direct result of the test and evaluation of the article or vehicle.
- Facilities, real property installed equipment, support equipment (e.g., provisions for storage, assembly, checkout, proof testing of hazardous systems/assemblies which may involve toxic, flammable, explosive, corrosive or cryogenic materials/wastes; radiation or noise emitters; electrical power sources) and training (e.g. training and certification pertaining to safety operations and maintenance).
- Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks; system redundancy; fail safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).
- Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.

DID MA-09 OPERATIONS HAZARD ANALYSIS AND HAZARD VERIFICATION TRACKING LOG

Title: Operations Hazard Analysis and Hazard Verification Tracking Log	DID No.: MA-09

MAR Paragraph: 3.3.3.2

Use:

The Operations Hazard Analysis (OHA) and Hazard Verification Tracking Log (VTL) shall demonstrate that hazards related to the operation of hardware and test equipment during integration and test activities have been addressed with respect to facility safety requirements.

Reference Documents:

- GSFC 500-PG-8715.1.2 AETD Safety Manual (for operations at GSFC)
- NASA-STD-8719.9 Standard for Lifting Devices and Equipment

Place/Time/Purpose of Delivery:

- Deliver the OHA and Hazard VTL for flight hardware to the Project Office forty-five (45) days prior to Pre-Environmental Review for approval (Note: OHA controls for engineering test units undergoing environmental tests shall be presented in accordance with local safety authorties 45 days prior to test performance)

Preparation Information:

The OHA shall include the following information:

- Introduction – a summary of the major findings of the analysis and the proposed corrective actions and definitions of special terms, acronyms, and abbreviations.
- System Description – a description of system hardware and configuration, with a list of subsystem components and schedules for integration and testing
- Analysis of Hazards
- List of real or potential hazards to personnel, equipment, and property during I&T processing
- The following information shall be included for each hazard:
  - System Component/Phase – the phase and component with which the analysis is concerned; e.g., system, subsystem, component, operating/maintenance procedure, or environmental condition.
  - System Description and Hazard Identification, Indication:
    - A description of expected results from operating the component/subsystem or performing the operating/maintenance action
    - A complete description of the actual or potential hazard resulting from normal actions or equipment failures; indicate whether the hazard will cause personnel injury and equipment damage.
    - A description of crew indications which include means of identifying the hazard to operating or maintenance personnel.
    - A description of the safety hazards of software controlling hardware systems where the hardware effects are safety critical.
  - Effect on System – the detrimental effects of an uncontrolled hazard on the system
  - Risk Assessment.
  - Caution and Warning Notes – a list of warnings, cautions, procedures required in operating and maintenance manuals, training courses, and test plans
  - Status/Remarks – the status of actions to implement hazard controls.
- References (e.g., test reports, preliminary operating and maintenance manuals, and other hazard analyses)

DID MA-10 SAFETY HAZARD ANALYSIS ON CRITICAL LIFT EQUIPMENT

Title: Safety Hazard Analysis for Critical Lift Equipment	DID No.: MA-10
MAR Paragraph: 3.3.3.3	
Use: A recognized safety hazard analysis, such as fault tree analysis, FMEA/FMECA, Operating and Support Hazard Analysis (O&SHA), shall be performed on all lifting devices used for critical lifts.	
Reference Documents: • NASA-STD-8719.9 Standard for Lifting Devices and Equipment, Para. 4.2.3, 5.2.3, 6.2.3, 8.2.3, 9.2.3, 11.2.3, 12.2.3, 13.2.3, and A.4.7	
Place/Time/Purpose of Delivery: • Deliver the analysis to the project office thirty (30) days prior to use in a critical lift for approval. • Deliver a revised analysis to the project office fifteen (15) days prior to use in a critical lift for approval.	
Preparation Information: The analysis shall determine potential sources of danger, identify failure modes, and recommend resolutions and a system of risk acceptance for those conditions found in the hardware-facility-environment-human relationship that could cause loss of life, personal injury, and loss of or damage to the crane, facility, or load.	

DID MA-11 OPERATING AND SUPPORT HAZARD ANALYSIS

Title: Operating and Support Hazard Analysis (O&SHA)	DID No.: MA-11
MAR Paragraph: 3.3.3.4	
Use: The Operating & Support Hazard Analysis (O&SHA) addresses hazards to personnel and equipment that are introduced via the usage of operational and support procedures during testing, transportation, storage, and integration operations at the launch site. Its primary purpose is to evaluate the adequacy of procedures used to eliminate, control or mitigate identified hazards in order to ensure implementation of safety requirements for personnel, procedures, and equipment used during testing, transportation, storage, and integration operations at the launch site.	
Reference Documents: • NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements • NPR 8715.7, ELV Payload Safety Program	
Place/Time/Purpose of Delivery: • Deliver the results of the O&SHA to the Project Office as a part of the SDP II & SDP III (DID MA-12) for approval	

DID MA-12 SAFETY DATA PACKAGE

Title: Safety Data Package (SDP)	DID No.: MA-12

MAR Paragraph: 3.3.4

Use:

The SDP provides a description of the design to support hazard analysis results, hazard analysis method, and other applicable safety related information. The developer shall include hazard analyses identifying the prelaunch, launch and flight hazards associated with the flight system, ground support equipment, and their interfaces. The developer shall take measures to control or minimize hazards.

In addition to identifying hazards, the SDP documents controls and verification methods for each hazard in Hazard Reports, which are included in a separate appendix. The analysis shall be updated as the hardware progresses through design, fabrication, and test. A list of hazardous/toxic materials with material safety data sheets and a description of the hazardous and safety critical operations associated with the payload shall be included in the final SDP.

The safety assessment shall begin early in the program formulation process and continue throughout all phases of the mission lifecycle through safe separation from the launch vehicle. The spacecraft Project Manager shall demonstrate compliance with these requirements and shall certify to NASA GSFC and the launch range, through the SDP, that all safety requirements have been met.

Reference Documents:

- NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements
- JSC 26943, Guidelines for the Preparation of Payload Flight Safety Data Packages and Hazard Reports

Place/Time/Purpose of Delivery:

- Deliver the SDP I to the Project Office forty-five (45) days prior to Mission PDR for approval.
- Deliver the SDP II to the Project Office forty-five (45) days prior to Mission CDR for approval.
- Deliver the SDP III to the Project Office ninety (90) days prior to shipment for approval.

NOTE: SDP I delivery shall include necessary launch range safety requirements tailoring (see DID MA-07).

Preparation Information:

1. Introduction. State the purpose of the safety data package.
2. System Description. This paragraph may be developed by referencing other program documentation such as technical manuals, System Program Plan, System Specification.
3. System Operations.
   a. A description of the procedures for operating, testing, and maintaining the system, including the safety features and controls.
   b. A description of special safety procedures needed to assure safe operations, test and maintenance, including emergency procedures.
   c. A description of anticipated operating environments and specific operator skills.
   d. A description of special facility requirements or personal equipment to support the system.
4. Systems Safety Engineering Assessment. This paragraph shall include:
   a. A summary of the criteria and methodology for classifying and ranking hazardous conditions.
   b. A description of the analyses and tests performed to identify inherent hazardous conditions, including the software safety analysis
   c. A separate appendix documenting the Hazard Reports by subsystem or major component level with the Hazard Reports being listed in alphanumeric order based on the chosen Hazard Report numbering scheme.
      i. A discussion of the actions taken to eliminate or control these items.

ii. A discussion of the effects of these controls in terms of fault tolerance, design for minimum risk, and severity level of potential mishaps.
iii. A discussion of the results of tests conducted to validate safety criteria requirements and analyses, including a reference to the specific test/analysis/inspection reports that provide this verification. These reports shall be made available to the Project office upon request.

5. Conclusions and Recommendations. This paragraph shall include:
   a. A list of significant hazards and specific safety controls.
   b. For hazardous materials:
      (1) Material identification as to type, quantity, and hazards.
      (2) Safety precautions and procedures for use, storage, transportation, and disposal.
      (3) A copy of the Material Safety Data Sheet (OSHA Form 20 or DD Form 1813).
   c. Appropriate radiation forms/analysis.
   d. Reference material to include a list of all pertinent references such as Test Reports, Preliminary Operating Manuals and Maintenance Manuals
   e. Recommendations applicable to the safe interface of this system with the other system(s).
   f. A statement signed by the developer's System Safety Manager and Program Manager certifying that all identified hazards have been eliminated or controlled and that the system is ready to test, operate, or proceed to the next acquisition phase.

DID MA-13 VERIFICATION TRACKING LOG

Title: SDP Verification Tracking Log	DID No.: MA-13
MAR Paragraph: 3.3.5	

Use:

Provides documentation of a Hazard Control and Verification Tracking process as a closed-loop system to ensure that safety compliance has been satisfied in accordance to applicable launch range safety requirements (related to the SDP).

Reference Documents:

- NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements

Place/Time/Purpose of Delivery:

- The Verification Tracking Log (VTL) that identifies hazard controls that are not verified as closed shall be delivered to the Project Office with the SDP III DID (MA-12) for review.
- Regular updates to this log shall be provided to the Project Office for review until all hazard controls are verified as closed.

Note: the developer shall close items with the appropriate verification rationale (e.g., test reports, analysis reports, procedure step references, etc.) prior to first use or to passing through an operational constraint.

Preparation Information:

The VTL provides documentation that demonstrates the process of verifying the control of all hazards by test, analysis, inspection, similarity to previously qualified hardware, or any combination of these activities. All verifications that are listed on the hazard reports shall reference the specific test/analysis/inspection reports with a summary of the pertinent results. Results of these tests/analyses/inspections shall be available for review and submitted in accordance with the contract schedule and applicable hazard report.

The VTL shall contain the following information in tabular format:

- Hazard Report number
- Safety Verification number
- Description (Identify procedures/analyses by number and title)
- Constraints on Launch Site Operations
- Independent Verification Required (e.g., mandatory inspection points)
- Scheduled Completion Date
- Completion Date
- Method of Closure

DID MA-14 HAZARDOUS PROCEDURES FOR PAYLOAD I&T AND PRE-LAUNCH PROCESSING

Title: Hazardous Procedures for Payload I&T and Pre-launch Processing	DID No.: MA-14
MAR Paragraph: 3.3.6	
Use: Documents hazardous procedures and associated safeguards that the developer will use for integration and test activities and pre-launch activities that comply with the applicable safety requirements of the installation where the activities are performed.	
Reference Documents: • GSFC 500-PG-8715.1.2 AETD Safety Manual (for GSFC I&T operations) • NASA-STD 8719.24 (with Annex), NASA Expendable Launch Vehicle Payload Safety Requirements • KNPR 8715.3, KSC Safety Practices Procedural Requirements (as applicable)	
Place/Time/Purpose of Delivery: • Submit Payload I&T Hazardous Procedures to the Project Office seven (7) days before first use for approval. • Submit Launch Range Hazardous Procedures to the Project Office sixty (60) days prior to first use for approval. • After Project Office approval, submit Launch Range Hazardous Procedures to Range Safety forty-five (45) days prior to first use for approval.	

DID MA-15 SAFETY WAIVER

Title: Safety Waiver	DID No.: MA-15
MAR Paragraph: 3.3.7	

Use:

A Safety Waiver documents a safety requirement that cannot be met and the rationale for approval of a waiver, as defined in NPR 8715.7. Note: a waiver request for relief from a SMA requirement may require Payload Safety Working Group (PSWG) concurrence.

Reference Documents:

- NPR 8715.7, ELV Payload Safety Program, Para. 1.5

Note: The waiver terminology and process defined in NPR 8715.7 is consistent with that of the launch range and payload processing community generally involved in NASA ELV payload missions. This consistency is considered essential to allow clear communication and resolution of waiver issues with the ELV payload community, which includes numerous organizations internal and external to NASA. There may be other Agency policy and terminology related to waivers that are exclusively internal to NASA. The ELV Payload Safety Program remains cognizant of NASA policy related to waivers and works with the payload projects and PSWGs to resolve any implementation concerns. In general, the Tailoring Process, coupled with the Waiver Process (defined by paragraphs 1.4 and 1.5 of NPR 8715.7), meet the overall intent of NASA policy to provide for appropriate oversight of Agency safety requirements while allowing the flexibility to accept reasonable risks necessary to accomplish ELV payload missions.

Place/Time/Purpose of Delivery:

- Deliver to the Project Office within thirty (30) days of identifying the need for a waiver for approval.

Preparation Information:

The developer shall include the following information from the review of a waiver request:

- A statement of the specific safety requirement and its associated source document name and paragraph number for which a waiver is requested.
- A technical justification for the waiver.
- Analyses to show the mishap potential of the proposed alternate requirement, method, or process as evaluated against the specified requirement.
- An assessment of the risk involved in accepting the waiver, including a list of all associated hazards and/or FMEA/FMECA/CILs; when it is determined that there are no hazards, the basis for such determination should be provided.
- A narrative on possible ways of reducing hazards severity and probability and existing compliance activities.
- Starting and expiration dates for waiver, if applicable.

DID MA-16 INPUT TO ORBITAL DEBRIS ASSESSMENT REPORT (ODAR) AND END OF MISSION PLAN (EOMP)

Title: Input to Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)	DID No.: MA-16
MAR Paragraph: 3.3.8	
Use: Ensure NASA requirements for post mission orbital debris control and end of mission planning are met.	
Reference Documents: • NASA-STD-8719.14 Process for Limiting Orbital Debris (Appendix A for ODAR, & Appendix B for EOMP	
Place/Time/Purpose of Delivery: • Deliver preliminary ODAR inputs to the Project Office fifteen (15) days prior to mission PDR for information. • Deliver ODAR interim inputs to the Project Office sixty (60) days prior to mission CDR for information. • Deliver the final/updated ODAR and EOMP inputs to the Project Office 90 days prior to PSR for information.	
Preparation Information: NASA-STD-8719.14 Process for Limiting Orbital Debris Appendix A (ODAR) and Appendix B (EOMP) provide details on what information is required for the Project Office to complete these analyses NOTE: Orbital Debris Assessment Software is available for download from Johnson Space Center at URL: http://sn-callisto.jsc.nasa.gov/mitigate/das/das.html	

DID MA-17 PRE-MISHAP PLAN

Title: Pre-Mishap Plan	DID No.: MA-17
MAR Paragraph: 3.3.9	

Use:

- Provides a plan for procedures to be followed to respond to and control a mishap or a close call that may have personnel or hardware safety implications, or may cause flight or GSE hardware damage.
- Provide the Project Office and NASA with information on any mishaps, incidents, and close calls related to the developer's efforts.

Reference Documents:

- Sample Pre-Mishap Plan – available from the Project Office upon request

Place/Time/Purpose of Delivery:

- Deliver to the Project Office forty-five (45) days prior to mission PDR for approval.

Preparation Information:

The plan shall identify the processes and procedures to be followed to respond to the occurrence of a mishap or a close call and identify the chain of individuals, including government personnel, to be contacted. The Mishap Plan should include the following information:

- The developer's policies and plan regarding response to a mishap or close call, to include:
  - Actions to be taken from the occurrence through implementation of corrective actions.
  - Plans for emergency response, notification, evidence preservation, mishap investigation, the mishap investigation report, lessons learned, and corrective actions.
  - Information regarding responsible for duties and tasks involved in the process.
- The following definitions:
  - Close Call -- An occurrence or a condition of employee concern in which there is no injury or minor injury requiring first aid and no or minor equipment or property damage (less than $2000) but which possesses a potential to cause a mishap.
  - Incident -- An occurrence of a close call or a mishap.
  - Mishap -- An unplanned occurrence that results in damage to property or personnel injury or illness: damage to developer, government, or customer-owned hardware property or critical products; fatalities, injuries, or illnesses occurring during program operations; environmental releases or spills occurring in the course of program operations.
- The following definitions regarding the type of mishaps:
  - Type A Mishap -- A mishap resulting in one or more of the following: (1) an occupational injury or illness resulting in a fatality, a permanent total disability, or the hospitalization for inpatient care of 3 or more people within 30 workdays of the mishap; (2) a total direct cost of mission failure and property damage of $2 million or more.
  - Type B Mishap -- A mishap that caused an occupational injury or illness that resulted in a permanent partial disability, the hospitalization for inpatient care of 1-2 people within 30 workdays of the mishap, or a total direct cost of mission failure and property damage of at least $500,000 but less than $2,000,000.
  - Type C Mishap -- A mishap resulting in a nonfatal occupational injury or illness that caused any days away from work, restricted duty, or transfer to another job beyond the day or shift on which it occurred, or a total direct cost of mission failure and property damage of at least $50,000 but less than $500,000.
  - Type D Mishap -- A mishap that caused any nonfatal OSHA recordable occupational injury and/or illness that does not meet the definition of a Type C mishap, or a total direct cost of mission failure and property damage of at least $2,000 but less than $50,000.
- Contact information for Project Office personnel.

- Notification schedule and mishap response process timeline (notification in no more than 24 hours).
- Note: The following are not reportable as mishaps but may be reportable as failures or anomalies:
  - Property Damage:
    - Items normally covered under Failure Reporting
    - Malfunction or failure of component parts or equipment due to normal wear and tear where the malfunction is the only damage and the only action is to replace or repair the equipment.
    - Anticipated damage to equipment or property was incurred during testing or manufacturing.
    - Property damage from vandalism, arson, sabotage or acts of God.
  - Injury:
    - Injuries and illnesses from non-occupational diseases.
    - Injuries that occur during work arrival or departure.
    - Injuries or illness sustained before working at the developer unless specifically aggravated by a work assignment.
    - Injuries from non-work-related, pre-existing disorders or by minimum stress and strain.
    - Injuries from activities unrelated to work (e.g., recreational activities, workouts, etc.).

DID MA-18 RANGE SAFETY FORMS

Title: Range Safety Forms	DID No.: MA-18
MAR Paragraph: 3.3.10	

Use:

Submitted to Launch Range Safety for assessment of range safety.

Reference Documents:

- KTI-5212 Material Selection List for Plastic Films, Foams, and Adhesive Tapes
- KNPR 1860.1 KSC Ionizing Radiation Protection Program
- KNPR 1860.2 KSC Non-Ionizing Radiation Protection Program

Place/Time/Purpose of Delivery:

- Deliver to the Project Office with the SDP III (DID MA-12) for review.

Preparation Information:

The developer shall complete the following forms:

- KTI-5212 Material Selection List for Plastic Films, Foams, and Adhesive Tapes
- KSC FORM 16-294 NS Radiation Training and Experience Summary (Ionizing Radiation)
- KSC FORM 16-295 NS Radiation Use Request/Authorization (Radiation Materials)
- KSC FORM 16-447 Laser Device Use Request/Authorization
- KSC FORM 16-450 NS Radiation Training & Experience Summary (Non-ionizing Radiation)
- KSC FORM 16-451 NS Radio Frequency/Microwave System Use Request/ Authorization
- KSC Form 26-551V2 Process Waste Questionnaire
- AF Form 813 Request for Environmental Impact Analysis

NOTE:

- Material Selection Forms are available for download from ELV Payload Safety Program website at URL: http://kscsma.ksc.nasa.gov/ELVPayloadSafety/NASAReferenceDocs_2 html
- Radiation Forms are available for download from ELV Payload Safety Program website at URL: http://kscsma.ksc.nasa.gov/ELVPayloadSafety/Forms.html

DID MA-19 RELIABILITY PROGRAM PLAN

Title: Reliability Program Plan	DID No.: MA-19
MAR Paragraph: 4.1	

Use:

Planning and implementation of Probabilistic Risk Assessment (PRA) and reliability activities.

Reference Documents:

- NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy
- NASA-STD-8729.1, Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program.
- NPR 8705.4 Risk Classification for NASA Payloads
- NPR 8705.5 PRA Procedures for NASA Programs and Projects

Place/Time/Purpose of Delivery:

- Deliver draft plan to the Project Office sixty (60) days after contract award for information.
- Deliver final plan to the Project Office thirty (30) days prior to the Systems Requirements Review for information.
- Deliver updates to the final plan to the Project Office thirty (30) days prior to implementation for information
- Deliver activity reports related to implementation of the plan at milestone reviews beginning with the Systems Requirements Review for approval.

Preparation Information:

The PRA and Reliability Program Plan shall include:

- A discussion of how the developer intends to implement and comply with PRA and Reliability program requirements.
- Charts and statements describing organizational responsibilities and functions conducting each task to be performed as part of the Program.
- A summary (matrix or other brief form) that indicates for each requirement, the organization responsible for implementing and generating the necessary documents.
- Identify the approval, oversight, or review authority for each task.
- Narrative descriptions, time or milestone schedules, and supporting documents describing the execution and management plan for each task.
- Documentation, methods, procedures, and reporting specific to each task in the plan.

DID MA-20: PROBABILISTIC RISK ASSESSMENT

Title: Probabilistic Risk Assessment	DID No.: MA-20
MAR Paragraph: 4.2	
Use: To provide a structured and disciplined approach to: analyzing system risk; supporting management decisions; improving safety, operations, performing maintenance and upgrades; improving performance; reducing costs.	
Reference Documents: • NPR 8705.4 Risk Classification for NASA Payloads • NPR 8705.5 Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects • NPR 8715.3 NASA General Safety Program Requirements • PRA Procedures Guide for NASA Managers and Practitioners (http://www.hq nasa.gov/office/codeq/doctree/praguide.pdf)	
Place/Time/Purpose of Delivery: • Deliver a PRA plan to the Project office sixty (60) days after contract award for review (Note: PRA may be stand-alone document or included as part of the Reliability Program Plan (RPP), Risk Management Plan (RMP), etc. The PRA Plan shall meet requirements delineated in DID MA-19.). • Deliver final plan to the Project Office thirty (30) days prior to the Systems Requirements Review for approval. • Deliver interim PRA to the Project Office thirty (30) days prior to PDR for review. • Deliver updated interim PRA to the Project Office thirty (30) days prior to CDR for review. • Deliver updated interim PRA to the Project Office thirty (30) days prior to MOR for review. • Deliver final PRA to the Project Office thirty (30) days prior to FOR for approval.	
Preparation Information: The PRA shall be performed in accordance with NPR 8705.5 and include the following: • The objective and scope of the PRA • End-states-of-interest to the decision-maker, • Definition of the mission phases and success criteria, • Initiating event categories, • Top level scenarios, • Initiating and pivotal event models (e.g., fault trees and phenomenological event models), including assessments of common cause failure modes • Data development for probability calculations, • Integrated model and quantification to obtain risk estimates, • Assessment of uncertainties, • Summary of results and conclusions, including a ranking of the lead contributors to risk.	

DID MA-21: FMEA/FMECA AND CRITICAL ITEMS LIST

Title: FMEA/FMECA and Critical Items List (CIL)	DID No.: MA-21

MAR Paragraph: 4.3

Use:

Used to evaluate design against requirements, to identify single point failures and hazards, and to identify modes of failure within a system design for the early mitigation of potential catastrophic and critical failures.

Reference Documents

- Code 322 Failure Mode and Effects Analysis guidance documentation
- Mil-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis
- NPR 8705.4 Risk Classification for NASA Payloads

Place/Time/Purpose of Delivery:

- Deliver preliminary FMEA/FMECA and CIL to the Project Office thirty (30) days before PDR for review.
- Deliver updated FMEA/FMECA and CIL to the Project Office thirty (30) days prior to CDR and each subsequent milestone review up to Launch Readiness Review for approval.

Preparation Information:

The FMEA/FMECA Report shall include the following:

- A discussion of the approach of the analysis, methodologies, assumptions, results, conclusions, and recommendations.
- Objectives
- Level of the analysis
- Ground rules
- Functional description
- Functional block diagrams
- Reliability block diagrams
- Equipment analyzed
- Data sources used
- Problems identified
- Corrective actions
- Work sheets identifying failure modes, causes, severity category, and effects at the item, next higher level, and mission level, detection methods, and mitigating provisions.
- Critical Items List (CIL) for severity categories 1, 1R, 1S, and 2, including item identification, cross-reference to FMEA/FMECA line items, and retention rationale. Appropriate retention rationale may include design features, historical performance, acceptance testing, manufacturing product assurance, elimination of undesirable failure modes, and failure detection methods.

DID MA-22: FAULT TREE ANALYSIS

Title: Fault Tree Analysis (FTA)	DID No.: MA-22

MAR Paragraph: 4.4

Use:

Used to assess mission failure from the top-level perspective. Undesired top-level states are identified and combinations of lower-level events are considered to derive credible failure scenarios. The technique provides a methodical approach to identify events or environments that can adversely affect mission success and provides an informed basis for assessing system risks.

Reference Documents

- NASA Fault Tree Handbook with Aerospace Applications (http://www.hq nasa.gov/office/codeq/doctree/fthb.pdf)
- NPR 8705.4 Risk Classification for NASA Payloads
- NPR 8715.3 NASA General Safety Program Requirements

Place/Time/Purpose of Delivery:

- Deliver preliminary qualitative mission FTA report to Project Office thirty (30) days prior to PDR for review.
- Deliver final qualitative mission FTA report to Project Office thirty (30) days prior to CDR for approval.
- Deliver qualitative mission FTA report to Project Office within thirty (30) days of updates/changes for approval.
- Deliver quantitative FTA report to Project Office in support of pivotal event analysis as part of each PRA report for approval.

Preparation Information:

The mission FTA Report shall contain:

- Analysis ground rules including definitions of undesirable end states
- References to documents and data used
- Fault tree diagrams
- Results and conclusions

Note: Separate FTA reports are not required for fault trees generated in support pivotal event analysis in the PRA report.

DID MA-23: PARTS STRESS ANALYSIS

Title: Parts Stress Analysis	DID No.: MA-23
MAR Paragraph: 4.5	

Use:

Provides EEE parts stress analyses for verifying circuit design conformance to derating requirements; demonstrates that environmental operational stresses on parts comply with project derating requirements.

Reference Documents

- GSFC EEE-INST-002 <http://nepp nasa.gov/DocUploads/FFB52B88-36AE-4378-A05B2C084B5EE2CC/EEE-INST-002_add1.pdf>
- NASA Parts Selection List <http://nepp.nasa.gov/npsl/index htm>

Place/Time/Purpose of Delivery:

- Deliver Parts Stress Analysis Report to Project Office forty-five (45) days prior to CDR for review.
- Deliver revisions to Parts Stress Analysis Report to the Project Office within thirty (30) days of changes for review.

Preparation Information:

The Parts Stress Analysis Report shall contain:

- Analysis ground rules
- Reference documents and data used
- Results and conclusions including:
  - Design trade study results
  - Parts stress analysis results impacting design or risk decisions
- Analysis worksheets; the worksheets at a minimum shall include:
  - Part identification (traceable to circuit diagrams)
  - Assumed environmental (consider all expected environments)
  - Rated stress
  - Applied stress (consider all significant operating parameter stresses at the extremes of anticipated environments)
  - Ratio of applied-to-rated stress

DID MA-24: WORST CASE ANALYSIS

Title: Worst Case Analysis	DID No.: MA-24
MAR Paragraph: 4.6	
Use: Demonstrate design margins in electronic and electrical circuits, optics, and electromechanical and mechanical items.	
Reference Documents • NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy. • NASA-STD-8729.1, Planning, Developing and Managing an Effective R&M Program. • NPR 8705.4, Risk Classification for NASA Payloads	
Place/Time/Purpose of Delivery: • Deliver Worst Case Analysis Report to Project Office thirty (30) days prior to CDR for review. • Deliver revisions to Worst Case Analysis Report to Project Office within thirty (30) days for review.	
Preparation Information: The Worst Case Analysis Report shall include the following: • Address worst case conditions performed on each component. • Discuss how each analysis includes the mission life. • Discuss consideration of critical parameters at maximum and minimum limits. • The effect of environmental stresses on the operational parameters being evaluated.	

DID MA-25: RELIABILITY ASSESSMENTS AND PREDICTIONS

Title: Reliability Assessments and Predictions	DID No.: MA-25

MAR Paragraph: 4.7

Use:

Used to assist in evaluating alternative designs and to identify potential mission limiting elements that may require special attention.

Reference Documents:

- MIL-STD-756B, Reliability Prediction
- MIL-HDBK-217, Reliability Prediction of Electronic Equipment
- MIL-HDBK-472, Maintainability Prediction
- SR-332 Issue 2, Reliability Prediction Procedure for Electronic Equipment, issued by Telcordia Technologies, September, 2006
- NSWC-07, The Handbook of Reliability Prediction Procedures for Mechanical Equipment, issued by the Naval Surface Warfare Center Carderock Division, July 31, 2007
- RIAC-HDBK-217Plus, Handbook of 217Plus Reliability Prediction Models
- IEC TR 62380 model is based on the Reliability Data Handbook - Universal Model for Reliability Prediction of Electronic Components, PCBs, and Equipment, published by the International Electrotechnical Commission (IEC)
- Chinese standard GJB/z 299B, Reliability Prediction Model for Electronic Equipment
- HRD5, Handbook for Reliability Data for Electronic Components used in Telecommunications Systems, Developed by British Telecommunications plc
- IEEE Std 1413-1998, IEEE Standard Methodology for Reliability Prediction and Assessment for Electronic Systems and Equipment
- Joseph G. Wohl, "Maintainability Prediction Revisited : Diagnostic Behavior, System Complexity, and Repair Time", IEEE Transactions On Systems, Man, And Cybernetics, Vol. SMC-12, No. 3, May/June 1982 pp. 241 – 250
- NASA/SP-2009-569 Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis

Place/Time/Purpose of Delivery:

- Deliver reliability assessment methodology to Project Office thirty (30) days prior to System Requirements Review for review.
- Deliver initial report Reliability Assessment and Prediction Report to Project Office thirty (30) days prior to PDR for review.
- Deliver revisions to the Reliability Assessment and Prediction Report to the Project Office thirty (30) days prior to CDR and each subsequent milestone review up to Launch Readiness Review for approval.

Preparation Information:

The Reliability Assessment and Prediction Report shall include the following:

- The methodology and results of comparative reliability assessments including mathematical models
- Reliability block diagrams
- Failure rates
- Failure definitions
- Degraded operating modes
- Trade-offs
- Assumptions
- Any other pertinent information used in the assessment process
- A discussion to show reliability was considered as a discriminator in the design process

DID MA-26 LIMITED-LIFE ITEMS LIST

Title: Limited-Life Items List	DID No.: MA-26
MAR Paragraph: 4.10	
Use: Tracks the selection and application of limited-life items and the predicted impact on mission operations.	
Reference Documents	
Place/Time/Purpose of Delivery: • Deliver Limited-Life Items List to the Project Office thirty (30) days prior to PDR for approval. • Deliver updates to the Limited-Life Items List to the Project Office no later than thirty (30) days after changes are made for approval.	
Preparation Information: The developer shall prepare and maintain a list of life-limited items and their predicted impact on mission operations. The list shall include expected life, required life, duty cycles, and rationale for selecting and using the item. The list may include such items as structures, thermal control surfaces, solar arrays, electromechanical mechanisms, batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, gyros, actuators and scan devices. The environmental or application factors that may affect the items include such things as atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue.	

DID MA-27: SOFTWARE ASSURANCE PLAN

Title: Software Assurance Plan	DID No.: MA-27

MAR Paragraph: 5.2

Use:

Documents the developer's software assurance roles and responsibilities and surveillance activities to be performed as outlined in the NASA Software Assurance Standard.

Reference Documents:

- NASA-STD-8739.8, NASA Standard for Software Assurance
- NASA-STD-8719.13, NASA Software Safety Standard
- IEEE Standard 730-2002, Software Quality Assurance Plans

Place/Time/Purpose of Delivery:

- Deliver preliminary plan to the Project Office thirty (30) days prior to SRR for information.
- Deliver final plan to the Project Office fifteen (15) days prior to PDR for information.
- Deliver updates to the Project Office fifteen (30) days prior to implementation for information.

Preparation Information:

The Software Assurance Plan (SAP) shall address the following:

- Purpose
- Scope
- Reference documents and definitions
- Assurance Organization and Management
- Assurance Activities by discipline
  - Software Quality (process and product)
  - Software Safety
  - Software Reliability
  - Software Verification and Validation
  - Independent Verification and Validation (if applicable)
- Assurance Activities for Complex Programmable Logic Devices (See note below)
- Assurance tools, techniques, and methodologies
- Software Assurance Program Metrics
- Problem Reporting and Corrective Action
- Assurance records, collection, maintenance, and retention
- Training
- Risk Management
- Requirements Compliance Matrix (NASA-STD-8739.8 Appendix C)
- SAP Change procedure and history

DID MA-28: SOFTWARE ASSURANCE STATUS REPORT

Title: Software Assurance Status Report	DID No.: MA-28

MAR Paragraph: 5.4

Use:

Software Assurance Status Report provides information regarding the developer's assurance activities, accomplishments, significant problems, and future plans.

Reference Documents:

- NASA-STD-8739.8, NASA Standard for Software Assurance
- NASA-STD-8719.13, NASA Software Safety Standard
- NPR 7150.2, NASA Software Engineering Requirements

Place/Time/Purpose of Delivery:

- Deliver to Project Office monthly beginning sixty (60) days after contract award for information.

Preparation Information:

Separately, or as part of the Project Monthly Status Reports, the developer shall status the following software assurance activities:

- Organization and key personnel changes
- Assurance accomplishments and resulting software assurance metrics (e.g., number of planned vs. actual audits/assessments, number of open vs. closed corrective actions resulting from audits)
- Subcontractor assurance accomplishments
- Trends in software quality metric data (e.g., total number of software problem reports, including the number of problem reports that were opened and closed in that reporting period)
- Significant problems or issues
- Plans for upcoming software assurance activities
- Recommendations and lessons learned

DID MA-29 RISK MANAGEMENT PLAN

Title: Risk Management Plan	DID No.: MA-29
MAR Paragraph: 7.1	

Use:

Defines the process by which the developer identifies, evaluates, and mitigates the risks associated with program, project, and/or mission goals

Reference Documents:

- NPR 8000.4, Risk Management Procedures and Guidelines

Place/Time/Purpose of Delivery:

- Deliver to the Project Office sixty (60) days after contract award for approval.

Preparation Information:

The Risk Management Plan shall include:

- Description of contract requirements
- Purpose and Scope
- Assumptions, Constraints, and Policies
- Reference Documents and Standards
- Risk Management Process Summary (Philosophy, Integration)
- Risk Management Organization
  - Roles and Responsibilities
  - Risk Management Review Board
  - Standard Practices
  - Communication
- Risk Attributes that will be used to classify risks
  - As a minimum attributes shall be defined for safety, cost, schedule, and technical or performance areas
- Risk buy-down chart (waterfall chart)
- Criteria for prioritization of risks
- Mitigation plan content
- Process Details
  - Baselines
  - Database (Use, Access, Updates, Responsibilities, etc.)
  - Identifying Risks
  - Analyzing Risks
  - Planning, Actions
  - Tracking (metrics and their use)
  - Control
  - Documentation
  - Reporting of Top Risks and Risk Data Charts

DID MA-30 RISK LIST

Title: Risk List	DID No.: MA-30
MAR Paragraph: 7.2	
Use: Defines the documentation and reporting of risk items.	
Reference Documents: • NPR 8000.4, Agency Risk Management Procedural Requirements	
Place/Time/Purpose of Delivery: • Deliver updated list to the Project Office monthly begining with PDR for review.	
Preparation Information: Prepare top risk list and risk data charts per the Risk Management Plan.	

DID MA-31 SYSTEMS REVIEW MATERIALS

Title: Systems Review Materials	DID No.: MA-31
MAR Paragraph: 8.1	
Use: To provide the systems review team with the materials used to conduct the review.	
Reference Documents • Project Systems Review Plan • GSFC-STD-1001 Criteria for Flight and Flight Support Systems Lifecycle Reviews. • NPR 7120.5 NASA Space Flight Program and Project Management Requirements, Section 2.2, Figure 2-5 • NPR 7123.1 NASA Systems Engineering Processes and Requirements, Chapter 5	
Place/Time/Purpose of Delivery: • Provide the review agenda to the Project Office fourteen (14) days prior to commencement of the review for information. • Provide the review presentation materials to the Project Office seven (7) days prior to the review for information. • Provide review related reference materials to the Project Office at the review for information.	
Preparation Information: See the guidelines presented in the reference documents.	

DID MA-32 ACTION ITEM RESPONSES

Title: Action Item Responses	DID No.: MA-32
MAR Paragraph: 8.1	
Use: To respond to action items resulting from the review.	
Reference Documents • Project Systems Review Plan (provided by Project Office) • GSFC-STD-1001 Criteria for Flight and Flight Support Systems Life-cycle Reviews	
Place/Time/Purpose of Delivery: • Provide an action item closure plan to the Project Office thirty (30) days after end of review for approval	
Preparation Information: See the guidelines presented in the related documents.	

DID MA-33 ENGINEERING PEER REVIEW PROGRAM

Title: Engineering Peer Review Program	DID No.: MA-33
MAR Paragraph: 8.2	
Use: To define the plan for conducting the developer's engineering peer review program.	
Reference Documents • GPR 8700.6 Engineering Peer Reviews	
Place/Time/Purpose of Delivery: • Provide to the Project Office sixty (60) days after contract award for review.	
Preparation Information: See the guidelines presented in the reference document.	

DID MA-34 SYSTEM PERFORMANCE VERIFICATION PLAN

Title: System Performance Verification Plan	DID No.: MA-34
MAR Paragraph: 9.1	
Use: Establishes the System Performance Verification Plan.	
Reference Documents: • GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects	
Place/Time/Purpose of Delivery: • Provide preliminary plan to Project Office thirty (30) days prior to PDR for review. • Provide final plan to Project Office thirty (30) days prior to CDR for approval.	
Preparation Information: The developer shall prepare and maintain a system performance verification plan that includes the tasks and methods to be used to verify the system's ability to meet mission level performance requirements. The requirements to be verified include those such as structural, thermal, optical, electrical, guidance and control, science, mission operations, etc. The developer shall also include alternatives to testing when there are limitations resulting from such situations as the 1-g environment, contamination control, voltage breakdown considerations, etc. The developer shall provide a risk assessment regarding the alternatives. The developer shall include a description of analysis activities, including objectives, a description of the models, assumptions, outputs, acceptance criteria, and interactions with test activities.	

DID MA-35 INTEGRATION, TEST, AND VERIFICATION PLAN

Title: Integration, Test, and Verification Plan	DID No.: MA-35
MAR Paragraph: 9.2	

Use:

To provide information on the integration, testing and verification activities. An overview of the entire I&T flow and its relation to performance verification. To describe the methods, policies, and organization, proto-flight and flight unit test program. The Contractor may submit separate plans for each phase of the test program as appendices or one plan covering all phases. To define the test requirements and the tests to be performed, instrumentation and locations, the tests methods, stimuli/measurements for acceptance criteria, and a time sequence for the testing.

This DID includes all the contractor generated documents necessary to perform the integration and testing of the instrument (e.g. the Environmental Verification Plan (EVP), the Environmental Test Matrix, GEVS verification, etc.). The EVP documents the contractor's approach for environmental qualification and acceptance tests.

Reference Documents:

- GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects

Place/Time/Purpose of Delivery:

- Provide preliminary plan to Project Office thirty (30) days prior to PDR for review.
- Provide updated plan to Project Office thirty (30) days prior to milestone reviews beginning with CDR for approval.

Preparation Information:

The developer shall provide an Integration and Test Plan which describes the series of activities required to integrate the various components into the final flight configuration. The developer shall prepare a test plan describing the methods, policies, and organization, proto-flight and flight unit test program. The plan shall also define the test requirements and the tests to be performed, instrumentation and locations, the tests methods, stimuli/measurements for acceptance criteria, and a time sequence for the testing.

Limitations in the verification program which preclude the verification by test of any system requirement shall be documented. Examples of limitations in the ability to demonstrate requirements include:

- Inability to deploy hardware in a 1-g environment.
- Facility limitations which do not allow testing at system level of assembly.
- Inability to perform certain tests because of contamination control requirements.
- Inability to perform powered-on testing because of voltage breakdown concerns.
- Alternative tests and analyses shall be evaluated and implemented as appropriate, and an assessment of program risk shall be included in the System Performance Verification Plan.

At a minimum, the plan shall contain the following information:

- Deliverables to integration and test
- Flow of integration and test sequence, including identification of calibration tests and characterizations. Identify instrument level requirements to be verified at each stage, cross referenced to the SPVP. Identify dependencies within the I&T sequence.
- Description of each instrument activity or test including the general test configuration
- Description of instrument procedures required to support the activity or test
- Description of simulated data/ simulator requirements

- Description of instrument special handling requirements to support the activity or test
- Description of instrument ground support equipment requirements to support the activity or test
- Description of instrument safety requirements to support the activity or test
- Description of instrument personnel required to support the activity or test
- Requirement to take photographs during the integration process for reference
- Description of the process to be used for handling anomalies as they occur during I&T
- Requirement of log books to be maintained throughout the I&T process

The developer shall prepare and maintain an environmental verification plan. The plan will include the overall approach to environmental verification; tests to be conducted at various levels of assembly, beginning with components; configuration of the item under test; test objectives; other considerations such as safety, facility requirements, contamination control, functional operations, and personnel.

DID MA-36 SYSTEM PERFORMANCE VERIFICATION MATRIX

Title: System Performance Verification Matrix	DID No.: MA-36
MAR Paragraph: 9.3	
Use: Establishes the System Performance Verification Matrix.	
Reference Documents: • GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects	
Place/Time/Purpose of Delivery: • The updated System Performance Verification Matrix shall be included with the review data package for milestone reviews beginning with PDR for review	
Preparation Information: The developer shall prepare and maintain a system performance verification matrix. The matrix will include: performance requirements and reference sources; method of compliance; procedure references; test results; report reference numbers.	

DID MA-37 INTEGRATION, TEST, AND VERIFICATION MATRIX

Title: Integration, Test, and Verification Matrix	DID No.: MA-37
MAR Paragraph: 9.4	
Use: Establishes a matrix that summarizes the environmental tests and test status for flight hardware and other equipment.	
Reference Documents: • GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects	
Place/Time/Purpose of Delivery: • The updated matrix shall be included with the review data package for milestone reviews beginning with PDR for review.	
Preparation Information: The developer shall prepare and maintain an environmental test matrix that includes the tests that will be performed on flight hardware beginning at the component level. The developer shall include sufficient details of each test so as to show that the hardware has been subjected to environmental exposures that demonstrate acceptable workmanship and that the test envirnonments relate to the mission environments. In addition, the matrix shall provide traceability of the qualification heritage of hardware. All flight hardware, spares and prototypes (when appropriate) shall be included in the matrix. Details of each test shall be provided (e.g., number of thermal cycles, temperature extremes, vibration levels). It shall also relate the design environments to the test environments and to the anticipated mission environments. The matrix shall be prepared in conjunction with the initial environmental verification plan and shall be updated as changes occur. A complementary matrix shall be included showing the tests that have been performed on each component or subsystem (or applicable level of assembly). This should include tests performed on prototypes or engineering units used in the qualification program, and should indicate test results (pass/fail or malfunctions).	

DID MA-38 VERIFICATION REPORTS

Title: Verification Reports	DID No.: MA-38
MAR Paragraph: 9.5	

Use:

Establishes the requirement to submit Verification Reports. Provides a summary of each integration and test result, conformance, non-conformance, and trend data. Establishes a Performance Verification Report that compares hardware/software specifications with the final verified values.

Reference Documents:

- GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects

Place/Time/Purpose of Delivery:

- Preliminary verification report shall be provided to Project Office within seventy-two (72) hours of test completion for information.
- Final verification report shall be provided to Project Office within thirty (30) days of test completion for information.
- Updated performance verification reports shall be provided with the review data package at milestone reviews, beginning with CDR, for information
- The final performance verification report shall be submitted within thirty (30) days after completion of on-orbit checkout for information

Preparation Information:

The developer shall submit a verification report after completion of verification activities at the component or higher level of assembly of flight hardware. The developer will include the following information in the report: project name; test item name or description; manufacturer; serial number: level of assembly; test description (including congiruation and GSE); procedure number; verification plan; facility and location; signature of cognizant engineer; signature of quality assurance representative; malfunction or nonconformance reports.

The reports should also include:

- Summary of the test results and an assessment of the quality and acceptability of the item tested, including pass/fail criteria and performance against the criteria.
- Trends in the performance of critical components
- Actual sequence of these operations including dates and times
- For thermal testing, tabulation of test target temperatures and actual test temperatures for all equipment and components along with the location of temperature Instruments used during the test
- For thermal balance testing, a tabulation of test prediction and actual temperatures and a tabulation of other pertinent targeted parameters vs. their actual test values, such as heater powers, heater place temperatures, solar intensity, etc.
- The document or a link to the document where the verification is recorded.

Contractor format may be used for these reports as long as the required information is included.

DID MA-39 ESD CONTROL PLAN

Title: ESD Control Plan	DID No.: MA-39
MAR Paragraph: 10.4	
Use: Implementation of an ESD control program at the developer's facility	
Reference Documents: • ANSI/ESD S20.20 For the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)	
Place/Time/Purpose of Delivery: • The developer shall submit an ESD Control Plan to the Project thirty (30) days prior to PDR for information.	
Preparation Information: The ESD Control Plan shall be prepared and implemented to comply with ANSI/ESD S20.20 requirements and the ESD sensitivity of the product being developed.	

DID MA-40 PARTS CONTROL PLAN (PCP)

Title: Parts Control Plan	DID No.: MA-40
MAR Paragraph: 11.1	

Use:

Development and implementation of an EEE parts control plan that addresses the system requirements for mission lifetime and reliability.

Reference Documents

- GSFC EEE-INST-002 Instructions for EEE Parts Selection, Screening, Qualification, and Derating
- S-311-M-70 Specification for Destructive Physical Analysis
- SAE AS5553 Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

Place/Time/Purpose of Delivery:

- The developer shall submit the PCP to the project office thirty (30) days after contract award for information.

Preparation Information:

The PCP shall address the following:

- Parts control program organization and management
- Shelf life control plan
- Parts application derating
- Supplier and manufacturer surveillance
- Qualification
- Procedures regarding application specific integrated circuits, gate arrays, system-on-chip, and custom integrated circuits
- Incoming inspection and test
- Sparing policies
- Destructive physical analysis
- Defective parts controls program.
- Handling, preservation, and packing
- Contamination control
- Alternate quality conformance inspection and small lot sampling
- Traceability and lot control
- Failure analysis
- Counterfeit parts control plan per AS5553
- Radiation hardness assurance program, which shall address: total ionizing dose; displacement damage (total non-ionizing dose); destructive and non-destructive single-event effects; single-event effect rates; proton hardness/tolerance

DID MA-41: PARTS CONTROL BOARD (PCB)

Title: Parts Control Board	DID No.: MA-41
MAR Paragraph: 11.2	
Use: Organization and operation of the Parts Control Board regarding the implementation of the Parts Control Program.	
Reference Documents:	
Place/Time/Purpose of Delivery: • The developer shall submit the Parts Control Board operating procedures to the project office thirty (30) days after contract award for information.	
Preparation Information: The developer shall address the following in the Parts Control Board procedures: • Organization and membership • Meeting schedule • Meeting notices • Distribution of meeting agenda, notes, and minutes • Review and approval responsibilities and processes	

DID MA-42 PARTS IDENTIFICATION LIST

Title: Parts Identification List (PIL)	DID No.: MA-42
MAR Paragraph: 11.3.1	
Use: A list of EEE parts that may be selected for use in flight hardware.	
Reference Documents:	
Place/Time/Purpose of Delivery: • The developer shall submit EEE parts to be added to the PIL to the Parts Control Board ten (10) business days prior to the first PCB meeting for approval by the PCB	
Preparation Information: The Parts Identification List shall contain the following information in a searchable electronic format: • Flight component identity to the circuit board level • Complete part number (i.e. Defense Supply Center Columbus part number, Specification Control Drawing part number, with all suffixes) • Manufacturer's Generic Part number • Manufacturer (not distributor) • Part Description (please include meaningful detail) • Federal Supply Class • Procurement Specification • Comments and clarifications, as appropriate • Estimated quantity required (for procurement forecasting)	

DID MA-43 PROJECT APPROVED PARTS LIST

Title: Project Approved Parts List (PAPL)	DID No.: MA-43
MAR Paragraph: 11.3.2	
Use: A list of EEE parts that are approved by the Parts Control Board for use in flight hardware.	
Reference Documents:	
Place/Time/Purpose of Delivery: • The developer shall submit EEE parts to be added to the Project Approved Parts List to the Parts Control Board ten (10) business days prior to the PCB meeting at which they will be presented for approval by the PCB	
Preparation Information: The PAPL shall contain all PIL fields plus the following information in a searchable electronic format: • Procurement Part Number • Flight Part Number (if different from the procurement part number) • Package Style/Designation • Single Event Latch-up (SEL) Hardness/Tolerance and Data Source • Single Event Upset (SEU) Hardness/Tolerance and Data Source • Total Ionizing Dose (TID) Hardness/Tolerance and Data Source • Displacement Damage Hardness/Tolerance (total non-ionizing dose) and Data Source • Proton Hardness/Tolerance and Data Source • PCB Status • PCB Approval Date • PCB Required Testing/Evaluations	

DID MA-44 AS DESIGNED PARTS LIST

Title: As Designed Parts List (ADPL)	DID No.: MA-44
MAR Paragraph: 11.3.3	
Use: A list of EEE parts that are designed into in flight hardware.	
Reference Documents	
Place/Time/Purpose of Delivery: • The developer shall submit EEE Parts to be added to the As Designed Parts List to the Parts Control Board ten (10) business days prior to the PCB meeting at which they will be presented for approval by the PCB	
Preparation Information: The As Designed Parts List (ADPL) shall contain all PAPL fields plus the following information in a searchable electronic format: • Assembly Name/Number • Next Level of Assembly • Need Quantity • Reference Designator(s) • Item number (if applicable)	

DID MA-45 AS BUILT PARTS LIST

Title: As Built Parts List (ABPL)	DID No.: MA-45
MAR Paragraph: 11.3.4	
Use: A list of EEE parts that are used in the flight hardware.	
Reference Documents	
Place/Time/Purpose of Delivery: • The developer shall submit EEE Parts to be added to the As Built Parts List to the Parts Control Board ten (10) business days prior to the PCB meeting at which they will be reviewed by the PCB	
Preparation Information: The As Built Parts List (ABPL): shall contain all ADPL fields plus the following information in a searchable electronic format: • Assembly serial number • Item revision • Next Level of Assembly serial number • Lot/Date/Batch/Heat/Manufacturing Code, as applicable • Manufacturer's Cage Code (specific plant location when relevant) • Distributor/supplier, if applicable • Part number • Part serial number (if applicable)	

DID MA-46 MATERIALS AND PROCESSES SELECTION, CONTROL, & IMPLEMENTATION PLAN

Title: Materials and Processes Selection, Control, & Implementation Plan	DID No.: MA-46

MAR Paragraph: 12.1

Use:

Defines the implementation of NASA-STD-6016 with prescribed changes as described in the Preparation Information.

Reference Documents:

NASA-STD-6016 Standard Materials and Processes Requirement for Spacecraft

Place/Time/Purpose of Delivery:

Provide to the Project Office sixty (60) days after contract award for approval.

Preparation Information:

For each paragraph in Section 4 of NASA-STD-6016, with the changes prescribed below, the plan shall state the requirement from NASA-STD-6016, identify the degree of conformance under the subheading "Degree of Conformance," and identify the method of implementation under the subheading "Method of Implementation."

The plan shall address the following:

- Conformance to the requirements of NASA-STD-6016 with the changes prescribed below and a description of the method of implementation.
- Organizational authority and responsibility for review and approval of M&P specified prior to release of engineering documentation.
- Identification and documentation of Materials and Processes
- Procedures and data documentation for proposed test programs to support materials screening and verification testing
- Materials Usage Agreement (MUA) Procedures
- Determination of material design properties, including statistical approaches to be employed.
- Identification of process specifications used to implement requirements in NASA-STD-6016.
- In addition to the requirements of paragraph 4.2.2.11, the developer shall meet the requirements of GEIA-STD-0005-1 and GEIA-STD-0005-2 for solders and surface finishes that are less than 3% lead by weight. The LFCP shall comply with the Level "2C" requirements set.
- In paragraph 4.1.2, the developer may use GFSC forms or the developer's equivalent forms in lieu of the MAPTIS format.
- The developer may use the GSFC outgassing database in addition to MAPTIS (URL http://outgassing.nasa.gov).

Prescribed changes to NASA-STD-6016:

- The developer shall use the NASA-STD-8719.24 NASA Expendable Launch Vehicle Payload Safety Requirements Table in place of paragraph 4.2.1.
- In addition to the requirements of paragraph 4.2.3.4, the developer shall qualify all lubricated mechanisms either by life testing in accordance with a life test plan or heritage with an identical mechanism used in an identical application. The developer shall perform a lubricant loss analysis for all mechanisms to show that the design meets a 10X margin (see DID MA-47).
- In addition to the requirements of paragraph 4.2.3.6, the developer shall provide the vacuum bake out schedule for materials that fail outgassing requirements with the MIUL or MUA.
- Paragraph 4.2.3.8 does not apply.
- In paragraph 4.2.5.1, the developer shall develop and implement a Non-Destructive Evaluation Plan only for fracture critical flight hardware (see DID MA-50).
- In paragraph 4.2.6.5, the developer shall use 541-PG-8072.1.2 GSFC Fastener Specification in place

of NASA-STD-6016.

- Paragraph 4.2.6.6 does not apply.

DID MA-47 LIFE TEST PLAN FOR LUBRICATED MECHANISMS

Title: Life Test Plan for Lubricated Mechanisms	DID No.: MA-47
MAR Paragraph: 12.2	
Use: Defines the life test evaluation process, acceptance criteria, and reporting for lubricated mechanisms.	
Reference Documents: • NASA-STD-6016 Standard Materials and Processes Requirement for Spacecraft • NASA-TM-86556 Lubrication Handbook for the Space Industry (Part A: Solid Lubricants, Part B: Liquid Lubricants) • NASA/CR-2005-213424 Lubrication for Space Applications	
Place/Time/Purpose of Delivery: • Provide plan to the Project thirty (30) days prior to PDR for approval. • Provide report to the Project thirty (30) days after acceptance test completion for review.	
Preparation Information: The Life Test Plan for Lubricated Mechanisms shall contain: • Table of Contents • Description of lubricated mechanisms, performance functions, summary of subsystem specification, and life requirements. • Heritage of identical mechanisms and descriptions of identical applications. • Design, drawings, and lubrication system used by the mechanism. • Test plan, including vacuum, temperature, and vibration test environmental conditions. • Criteria for a successful test. • Final report.	

DID MA-48 MATERIALS USAGE AGREEMENT

Title: Materials Usage Agreement (MUA)	DID No.: MA-48
MAR Paragraph: 12.3	
Use: Establishes the process for submitting a MUA for a material or process that does not meet the requirements of NASA-STD-6016 and does not affect reliability or safety when used per the Materials and Processes Selection, Control, and Implementation Plan.	
Reference Documents: • NASA-STD-6016 Standard Materials and Processes Requirement for Spacecraft • MSFC-STD-3029 Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments	
Place/Time/Purpose of Delivery: • Provide new MUAs to the Project thirty (30) days prior to CDR for approval. • After the initial submission of MUAs, revised MUAs shall be provided to the Project within thirty (30) days of their identification for approval.	
Preparation Information: The MUA system shall be defined in the Materials and Processes Selection, Control, and Implementation Plan as approved per paragraph 1.2 (see DID MA-46). The MUA package shall include the technical information required to justify the application. MUAs for stress corrosion shall include a Stress Corrosion Cracking Evaluation Form per MSFC-STD-3029 (see NASA-STD-6016) and a stress analysis.	

DID MA-49 MATERIALS IDENTIFICATION AND USAGE LIST

Title: Materials Identification and Usage List (MIUL)	DID No.: MA-49
MAR Paragraph: 12.4	
Use: Establishes the Materials Identification and Usage List (MIUL).	
Reference Documents: • NASA-STD-6016 Standard Materials and Processes Requirement for Spacecraft	
Place/Time/Purpose of Delivery: • Provide to the Project Office thirty (30) days prior to PDR for review • Provide to the Project Office thirty (30) days prior to CDR approval • Provide updates to the Project Office within thirty (30) days of identification for review	
Preparation Information: The MIUL documenation approach shall be defined in the Materials and Processes Selection, Control, and Implementation Plan as approved per paragraph 1.2 (see DID MA-46).	

DID MA-50_NONDESTRUCTIVE EVALUATION PLAN

Title: Nondestructive Evaluation Plan	DID No.: MA-50
MAR Paragraph: 12.5	

Use:

Establishes the Non-Destructive Evaluation (NDE) plan for the procedures and specifications employed in the inspection of materials.

Reference Documents:

- NASA-STD-6016 Standard Materials and Processes Requirement for Spacecraft
- MIL-HDBK-6870, Inspection Program Requirements, Nondestructive for Aircraft and Missile Materials and Parts
- NASA-STD-5009 Nondestructive Evaluation Requirements for Fracture-Critical Metallic Components

Place/Time/Purpose of Delivery:

- Provide to the Project thirty (30) days prior to PDR for review.
- Provide to the Project thirty (30) days prior to CDR for approval.
- Provide updates to the Project thirty (30) days after identification for approval.

Preparation Information:

The NDE Plan shall describe the process for establishment, implementation, execution and control of NDE. The plan shall meet the intent of MIL-HDBK-6870, Inspection Program Requirements, Nondestructive for Aircraft and Missile Materials and Parts and NASA-STD-5009 Nondestructive Evaluation Requirements for Fracture-Critical Metallic Components, as specified by NASA-STD-6016.

The plan shall define NDT planning and requirements to include the following:

- Hardware Design
- Manufacturing Planning
- Personnel Training
- NDE Reliability Requirements for Fracture Critical Parts
- NDE Reporting

DID MA-51 PRINTED WIRING BOARDS TEST COUPONS

Title: Printed Wiring Board (PWB) Test Coupons	DID No.: MA-51
MAR Paragraph: 12.6	

Use:

PWB test coupons are evaluated to validate that PWBs are suitable for use in space flight and mission critical ground applications.

Reference Documents:

- IPC-6011 Generic Performance Specifications for Printed Boards (Class 3 Requirements)
- IPC-6012B Qualification and Performance Specification for Rigid Printed Boards (Class 3/A Requirements/Performance Specification Sheet for Space and Military Avionics)
- IPC-6013 Qualification and Performance Specification for Flexible Printed Boards (Class 3 Requirements)
- IPC-6018 Qualification and Performance Specification for High Frequency (Microwave) Printed Boards (Class 3 Requirements)
- IPC A-600 Guidelines for Acceptability of Printed Boards
- IPC-2221 Generic Standard on Printed Board Design

Place/Time/Purpose of Delivery:

- The developer shall deliver test coupons and supporting manufacturing information traceable to the flight boards to GSFC or a GSFC approved laboratory as soon as practicable for analysis of the printed wiring boards for approval.
- The developer shall notify GSFC regarding shipment of PWB test coupons as it occurs for information.

Note: Coupon specimens do not need to be submitted for single-sided PWBs.

Note: If a GSFC-approved laboratory is used for coupon evaluation, the developer shall deliver the laboratory results to GSFC as part of the end item data package per Section 16 and DID MA-56.

Preparation Information:

The developer shall provide:

- Coupon specimens with sufficient A, B, A/B coupons, or their equivalent per IPC-2221 for both unstressed and thermally stressed micro sectioned coupon evaluation per section 3.6 of the applicable IPC-60XX specification.
- If the represented PWB design contains a blind, buried, or micro via, the developer shall provide additional B or A/B coupons for each contained feature for thermally stressed evaluation.
- M coupon or equivalent if a specialty plating is used (e.g., ENIG, ENIPIG).
- Supporting manufacturing documentation that is traceable to the flight boards and that includes: the specification to which the board was produced; board drawing or drawing notes; class of printed board; type of printed board; indication if there are blind, buried, or micro vias present; laminate information; part number; serial number and Vendor ID (CAGE Code for a US manufacturer).

DID MA-52 CONTAMINATION CONTROL PLAN AND DATA

Title: Contamination Control Plan and Data	DID No.: MA-52
MAR Paragraph: 13.1	

Use:

To establish contamination allowances, methods for controlling contamination, and record test results

Reference Documents:

- GSFC-STD-7000 General Environmental Verification Standard (GEVS)
- GSFC-STD-1000 Rules for the Design, Development, Verification, and Operation of Flight Systems
- ASTM E595 Standard Test Methods for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment
- Outgassing Data for Selecting Spacecraft Materials (URL: http://outgassing.nasa.gov/)

Place/Time/Purpose of Delivery:

- Provide to the Project Office thirty (30) days before PDR for GSFC review.
- Provide to the Project Office thirty (30) days before the CDR for approval.
- Final thermal vacuum bakeout results provided to the Project Office within thirty (30) of completion for review.
- Provide contamination certificate of compliance with End Item Acceptance Data Package (DID MA-56) for review

Preparation Information:

The developer shall provide: material properties data; design features; test data; system tolerance of degraded performance; methods to prevent degradation. The items below shall be addressed in the plan:

- Beginning of life and end of life requirements for contamination sensitive surfaces or subsystems
- Methods and procedures used to measure and maintain the levels of cleanliness required during each of the various phases of the item's lifetime (e.g., protective covers, environmental constraints, purges, cleaning/monitoring procedures)
- Materials
  - Outgassing as a function of temperature and time.
  - Nature of outgassing chemistry.
  - Areas, weight, location, view factors of critical surfaces.
- Venting: size, location and relation to external surfaces.
- Thermal vacuum test contamination monitoring plan, to include vacuum test data, QCM location and temperature, pressure data, system temperature profile, and shroud temperature.
- On-orbit spacecraft and instrument performance as affected by contamination deposits.
  - Contamination effect monitor
  - Methods to prevent and recover from contamination in orbit
  - Evaluation of on-orbit degradation
  - Photopolymerization of outgassing products on critical surfaces
  - Space debris risks and protection
  - Atomic oxygen erosion and re-deposition
- Analysis of contamination impact on the satellite on orbit performance
- In orbit contamination impact from other sources such as STS, space station, and adjacent instruments
- Ground/Test support equipment controls to prevent contamination of flight item(s)
- Facility controls and processes to maintain hardware integrity (protection and avoidance)
- Training
- Data package on test results for materials and as-built product

DID MA-53 FOREIGN OBJECT DEBRIS PREVENTION AND CONTROL PLAN

Title: Foreign Object Debris Prevention and Control Plan	DID No.: MA-53
MAR Paragraph: 13.2	
Use: The plan will provide guidance regarding the prevention and control of foreign object debris with respect to the flight hardware.	
Reference Documents: • NAS 412 Foreign Object Damage/Foreigh Object Debris (FOD) Prevention	
Place/Time/Purpose of Delivery: • Provide to the Project Office thirty (30) days before PDR for review	
Preparation Information: The plan will address the preservation of product with respect to foreign object debris prevention per the requirements of NAS 412.	

DID MA-54 GIDEP ALERT / NASA ADVISORY DISPOSITIONS

Title: GIDEP Alert / NASA Advisory Dispositions	DID No.: MA-54
MAR Paragraph: 15.2	

Use:

Document the developer's disposition of GIDEP ALERTs; GIDEP SAFE-ALERTs; GIDEP Problem Advisories; GIDEP Agency Action Notices; NASA Advisories and component issues, hereinafter referred to collectively as "Alerts" with respect to parts and materials, equipment, and software used in NASA products.

Reference Documents:

- GIDEP Operations Manual (SO300- BT-PRO-010)
- GIDEP Requirements Guide (S0300-BU-GYD-010)

Place/Time/Purpose of Delivery:

- Provide disposition of existing Alerts to the Project Office within 30 days of identification of potential use or use of an EEE part, material, equipment, or software for review.
- Provide disposition of new Alerts to the Project Office for EEE parts, materials, equipment, or software already approved for use within 30 days of Alert release date for review.

Preparation Information:

The developer shall submit:

- A completed GSFC Form 4-37, "Problem Impact Statement Parts, Materials and Safety", GSFC Form 4-37A "Problem Impact Statement Safety-Related Documents", or equivalent developer form, for each Alert.

Note: Use-as-is dispositions for parts, materials, equipment, or software directly impacted by an Alert require thorough documentation, including documented concurrence from discipline areas contributing to the response and supporting objective evidence, such as thermal, or worst case circuit stress, or environmental stress analyses.

DID MA-55 SIGNIFICANT PARTS, MATERIALS, AND SAFETY PROBLEMS

Title: Significant parts, materials, and safety problems	DID No.: MA-55
MAR Paragraph: 15.3	
Use: Document the developer's identification of significant parts, material, and safety problems and the developer's actions as required by the GIDEP manual regarding the decision to prepare an Alert, including the type of Alert that is applicable.	
Reference Documents: • GIDEP Operations Manual (SO300- BT-PRO-010) • GIDEP Requirements Guide (S0300-BU-GYD-010)	
Place/Time/Purpose of Delivery: • Deliver to the Project Office within thirty (30) days of identification for review.	
Preparation Information: The developer shall submit relevant information (e.g., failure analyses, test reports, root cause and corrective action evaluations).	

DID MA-56 END ITEM ACCEPTANCE DATA PACKAGE

Title: End Item Acceptance Data Package	DID No.: MA-56
MAR Paragraph: 16	

Use:

The End Item Acceptance Data Package documents the design, fabrication, assembly, test, and integration of the hardware and software being delivered and is included with the end item delivery.

Reference Documents:

Place/Time/Purpose of Delivery:

- Provide the End Item Acceptance Data Package to the Project thirty (30) days prior to end item delivery for approval.

Preparation Information:

The developer prepares the End Item Acceptance Data Package as part of design development and implementation such that it is completed prior to delivery. The following items shall be included:

- The deliverable item name, serial number, part number, and classification status (e.g., flight, non-flight, ground support)
- Appropriate approval signatures (e.g., developer's quality representative, product design lead, government Representative)
- List of shortages or open items at the time of acceptance with supporting rationale
- As-built serialization
- As-built configuration
- In-process Work Orders (available for review at developers--not a deliverable)
- Final assembly and test Work Order
- Major MRB actions
- Major anomaly reports
- Acceptance testing procedures and report(s), including environmental testing
- Trend data
- Anomaly/problem failure reports with root cause and corrective action dispositions
- As-built EEE parts list
- As-built materials list
- Chronological history, including:
  - Total operating hours and failure-free hours of operation
  - Total number of mechanical cycles and remaining cycle life
- Limited life items, including data regarding the life used and remaining
- As-built final assembly drawings
- PWB coupon results
- Photographic documentation of hardware (pre and post-conformal coating for printed wiring assemblies, box or unit, subsystem, system, harness, structure, etc.)
- Waivers
- Certificate of Compliance which is signed by management

Appendix C. MAR Response Form

- Enter *Yes* or *No* regarding compliance with the requirements.
- A response of *Yes* indicates full compliance with the requirements. The Comment column should be used as required to indicate how compliance will be achieved, e.g., through an equivalent procedure.
- A response of *No* indicates less than full compliance with the requirements and requires an entry in the Comment column to explain the deviation from full compliance.

Paragraph or DID	Title	Comply Y / N	Comment (Required for *No*)
1 General			
1.1	Systems Safety and Mission Assurance Program		
1.2	Management		
1.3	Requirements Flowdown		
1.4	Suspension of Work Activities		
1.5	Contract Data Requirements List		
1.6	Surveillance		
1.7	Use of Previously Developed Product		
DID MA-01	Mission Assurance Implementation Plan		
DID MA-02	Previously Developed Product – Compliance with Requirements		
2 Quality Management System			
2.1	General		
2.2	Supplemental Quality Management System Requirements		
2.2.1	Control of Nonconforming Product		
2.2.2	Material Review Board		
2.2.3	Anomaly Reporting and Disposition		
DID MA-03	Reporting of MRB Actions		
DID MA-04	Request for a Waiver		
DID MA-05	Anomaly Report		
3 System Safety			
3.1	General		
3.2	Mission Related Safety Requirements Documentation		
3.3	System Safety Deliverables		
3.3.1	System Safety Program Plan		
3.3.2	Safety Requirements Compliance Checklist		
3.3.3	Hazard Analyses		
3.3.3.1	Preliminary Hazard Analysis		
3.3.3.2	Operations Hazard Analysis (OHA) and Hazard Verification Tracking Log (VTL)		
3.3.3.3	Lifting Devices Safety Requirements		
3.3.3.4	Operating and Support Hazard Analysis		
3.3.4	Instrument Safety Assessment Report ***Or*** Safety Data Package		
3.3.5	Verification Tracking Log		
3.3.6	Hazardous Procedures for Payload I&T and Pre-Launch Processing		
3.3.7	Safety Waivers		
3.3.8	Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)		

Paragraph or DID	Title	Comply Y / N	Comment (Required for *No*)
3.3.9	Mishap Reporting and Investigation		
3.3.10	Range Safety Forms		
DID MA-06	System Safety Program Plan		
DID MA-07	Safety Requirements Compliance Checklist		
DID MA-08	Preliminary Hazard Analysis		
DID MA-09	Operations Hazard Analysis		
DID MA-10	Safety Hazard Analysis on Critical Lift Equipment		
DID MA-11	Operating and Support Hazard Analysis		
DID MA-12	Safety Data Package		
DID MA-13	SDP Verification Tracking Log		
DID MA-14	Hazardous Procedures for Payload I&T and Pre-Launch Processing		
DID MA-15	Safety Waivers		
DID MA-16	Input to Orbital Debris Assessment Report and End of Mission Plan		
DID MA-17	Pre-Mishap Plan		
DID MA-18	Range Safety Forms		
4 Probablistic Risk Assessment and Reliability			
4.1	Reliability Program Plan		
4.2	Probabilistic Risk Assessment (PRA)		
4.3	Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)		
4.4	Fault Tree Analysis		
4.5	Parts Stress Analysis		
4.6	Worst Case Analysis		
4.7	Reliability Assessments and Predictions		
4.8	Limited Life Items		
MA-19	Reliability Program Plan		
MA-20	Probabilistic Risk Assessment (PRA) ***or*** Input to Probabilistic Risk Assessment (PRA)		
DID MA-21	FMEA/FMECA and Critical Items List		
DID MA-22	Fault Tree Analysis		
DID MA-23	Parts Stress Analysis		
DID MA-24	Worst Case Analysis		
DID MA-25	Reliability Assessments and Predictions		
DID MA-26	Limited-Life Items List		
5 Software Assurance (Flight and Ground Segments)			
5.1	Applicable Software Definintion		
5.2	Software Assurance Program		
5.2.1	Software Quality		
5.2.2	Software Safety Analysis		
5.2.3	Software Reliability Analysis		
5.2.4	Verification and Validation		
5.2.5	Independent Verification and Validation		
5.3	Reviews		
5.4	Surveillance of Software Development, Maintenance, and Assurance Activities		
DID MA-27	Software Assurance Plan		

Paragraph or DID	Title	Comply Y / N	Comment (Required for *No*)
DID MA-28	Software Assurance Status Report		
6 Digital Electronic Components			
6.1	General		
6.2	Peeer Reviews		
7 Risk Management			
7.1	General		
7.2	Risk List		
MA-29	Risk Management Plan		
MA-30	Risk List		
8 Systems Reviews			
8.1	Systems Reviews		
8.2	Peer Reviews		
DID MA-31	Systems Review Materials		
DID MA-32	Action Item Responses		
DID MA-33	Engineering Peer Review Program		
9 System Performance Verification			
9.1	System Performance Verification Program Plan		
9.2	Environmental Verificaton Plan		
9.3	System Performance Verification Matrix		
9.4	Environmental Test Matrix		
9.5	Verification Reports		
9.6	System Performance Verification Report		
DID MA-34	System Performance Verification Plan		
DID MA-35	Integration, Test, and Verification Plan		
DID MA-36	System Performance Verification Matrix		
DID MA-37	Integration, Test, and Verification Matrix		
DID MA-38	Verification Reports		
10 Workmanship			
10.1	General		
10.2	Design and Process Qualification		
10.3	Electrostatic Discharge Control (ESD)		
10.4	Splices, Circuit Board Trace Cuts, and Jumper Wires		
10.5	Re-use of EEE parts and materials		
DID MA-39	ESD Control Plan		
11 EEE Parts			
11.1	General		
11.2	Parts Control Board		
11.3	EEE Parts Lists		
11.3.1	Parts Identification List (PIL)		
11.3.2	Project Approved Parts List (PAPL)		
11.3.3	As-Designed Parts List (ADPL)		
11.3.4	As-Built Parts List (ABPL)		
DID MA-40	Parts Control Plan		
DID MA-41	Parts Control Board		
DID MA-42	Parts Identification List		
DID MA-43	Project Approved Parts List		
DID MA-44	As Designed Parts List		

Paragraph or DID	Title	Comply Y / N	Comment (Required for *No*)
DID MA-45	As Built Parts List		
12 Materials and Processes			
12.1	General		
12.2	Life Test Plan for Lubricated Mechanisms		
12.3	Materials Usage Agreement (MUL)		
12.4	Materials Identification and Usage List (MIUL)		
12.5	Nondestructive Evaluation Plan (NDE)		
12.6	Printed Wiring Board Test Coupons		
12.7	Titanium Alloys		
DID MA-46	Materials & Processes Selection, Control, and Implementation		
DID MA-47	Life Test Plan for Lubricated Mechanisms		
DID MA-48	Materials Usage Agreement		
DID MA-49	Materials Identification and Usage List		
DID MA-50	Nondestructive Evaluation Plan		
DID MA-51	Printed Wiring Boards Test Coupons		
13 Contamination Control			
13.1	Contamination Control Plan		
DID MA-52	Contamination Control Plan and Data		
13.2	Foreign Object Debris Program		
DID MA-53	Foreign Object Debris Prevention and Control Plan		
14 Metrology and Calibration			
14.1	Metrology and Calibration Program		
14.2	Use of Non-calibrated Instruments		
15 GIDEP Alerts and Problem Advisories			
15.1	Government-Industry Data Exchange Program (GIDEP)		
15.2	Alert Disposition		
15.3	GIDEP Reporting		
15.4	Review Reporting		
DID MA-54	GIDEP Alert and NASA Advisory Dispositions		
DID MA-55	Significant Parts, Materials, and Safety Problems		
16 End Item Acceptance Data Package			
16	End Item Acceptance Data Package		
DID MA-56	End Item Acceptance Data Package		

Appendix D. Data Item Description List

DID #	MAR Paragraph	Title	Due	Purpose
MA-01	1.1	Mission Assurance Implementation Plan	1. 60 days after contract award 2. Updates thirty (30) days prior to implementation	Approval
MA-02	1.7	Previously Developed Product – Compliance with Requirements	30 days after identification of previously developed product	Approval
MA-03	2.2.2	Reporting of MRB Actions	3. Major MRB actions: within five (5) working days of MRB action 4. Minor MRB actions: within five (5) working days of MRB action	1. Approval 2. Review
MA-04	2.2.2	Request for a Waiver	Within five (5) working days of identifying the need for a waiver	Approval
MA-05	2.2.3	Major Anomaly Report	1. Initial submission to the project office within 24 hours of occurrence 2. Notice of a change in status within 24 hours of occurrence 3. Proposed closure to the project office prior to closure	1. Information 2. Information 3. Approval
MA-06	3.3.1	System Safety Program Plan	1. Preliminary to the Project Office at SRR. 2. Final to the Project Office forty-five (45) days prior to PDR 3. Updates thirty (30) days prior to implementation	Information
MA-07	3.3.2	Safety Requirements Compliance Checklist	1. Prelminary to the Project Office forty-five (45) days prior to PDR. 2. Deliver Final to the Project Office forty-five (45) days prior to CDR.	Approval
MA-08	3.3.3.1	Preliminary Hazard Analysis	As a part of the SDP I (DID MA-12)	Approval
MA-09	3.3.3.2	Operations Hazard Analysis	Deliver the OHA and Hazard Verification Tracking Log to the Project Office forty-five (45) days prior to Systems Integration Review or Pre-Environmental Review	Approval
MA-10	3.3.3.3	Safety Hazard Analysis on Critical Lift Equipment	1. Deliver the analysis to the project office thirty (30) days prior to use in a critical lift for approval. 2. Deliver a revised analysis to the project office fifteen (15) days prior to use in a critical lift for approval.	Approval
MA-11	3.3.3.4	Operating and Support Hazard Analysis	1. As a part of the SDP II & SDP III (DID MA-12)	Approval

DID #	MAR Paragraph	Title	Due	Purpose
MA-12	3.3.4	Safety Data Package	1. SDP I 45 days prior to Mission PDR 2. SDP II 45 days prior to Mission CDR 3. SDP III 90 days prior to shipment	Approval
MA-13	3.3.5	SDP Verification Tracking Log	1. Hazard controls not verified as closed with the final ISAR (DID MA-12) 2. Hazard controls not verified as closed with the SDP III DID (MA-12) 3. Regular updates provided until all hazard controls are verified as closed.	Review
MA-14	3.3.6	Hazardous Procedures for Payload I&T and Pre-Launch Processing	1. I&T hazardous procedures to Project Office 7 days before first use 2. Launch Range Hazardous Procedures to the Project Office 60 days prior to first use 3. Launch Range Hazardous Procedures to Range Safety forty-five (45) days prior to first use (after NASA approval)	Approval
MA-15	3.3.7	Safety Waivers	Within thirty (30) days of identifying the need for a waiver	Approval
MA-16	3.3.8	Input to Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)	1. Deliver preliminary ODAR inputs to the Project Office fifteen (15) days prior to mission PDR for information. 2. Deliver ODAR interim inputs to the Project Office sixty (60) days prior to mission CDR for information. 3. Deliver the final/updated ODAR and EOMP inputs to the Project Office 90 days prior to PSR for information.	Information
MA-17	3.3.9	Pre-Mishap Plan	45 days prior to mission PDR	Approval
MA-18	3.3.10	Range Safety Forms	1. With SDP III (DID MA-12)	Review
MA-19	4.1	Reliability Program Plan	1. Sixty (60) days after contract award 2. Final plan 30 days prior to the Systems Requirements Review 3. Activity reports at milestone reviews beginning with the Systems Requirements Review	1. Information 2. Information 3. Information

DID #	MAR Paragraph	Title	Due	Purpose
MA-20*	4.2	Probabilistic Risk Assessment	1. Deliver a PRA plan to the Project office sixty (60) days after contract award 2. Deliver interim PRA to the Project Office thirty (30) days prior to PDR. 3. Deliver updated interim PRA to the Project Office thirty (30) days prior to CDR. 4. Deliver updated interim PRA to the Project Office thirty (30) days prior to MOR. 5. Deliver final PRA to the Project Office thirty (30) days prior to FOR.	1. Review 2. Review 3. Review 4. Review 5. Approval
MA-20	4.2	Input to the Probalistic Risk assessment (PRA)	1. Deliver preliminary heritage information, including the percent applicable, to the Project Office sixty (60) days after contract award. 2. Deliver updated heritage information, including the percent applicable heritage to the subject mission, to the Project Office thirty (30) days to prior major milestone reviews beginning with the SRR. 3. Deliver product information and process information for elements within the scope of the Mission PRA to the Project Office thirty (90) days prior to the PDR and thirty (30) days prior to subsequent major milestone reviews.	Information
MA-21	4.3	FMEA/FMECA and Critical Items List	1. Preliminary FMEA/FMECA thirty (30) days before PDR 2. Final FMEA/FMECA thirty (30) days prior to CDR 3. Updated FMEA/FMECA and CIL thirty (30) days prior to each subsequent milestone review leading up to Launch	1. Review 2. Approval 3. Approval
MA-22	4.4	Fault Tree Analysis	1. Preliminary qualitative FTA report thirty (30) days prior to PDR 2. Final qualitative FTA report thirty (30) days prior to CDR 3. Updated qualitative FTA report thirty (30) days of updates/changes 4. Final quantitative FTA report in support of pivotal event analysis as part of each PRA report	1. Review 2. Approval 3. Approval 4. Approval

DID #	MAR Paragraph	Title	Due	Purpose
MA-23	4.5	Parts Stress Analysis	1. Forty-five (45) days prior to CDR 2. Revisions within thirty (30) days	Review
MA-24	4.6	Worst Case Analysis	1. Thirty (30) days prior to CDR 2. Revisions within thirty (30) days	Review
MA-25	4.7	Reliability Assessments and Predictions	1. Methodology thirty (30) days prior to System Requirements Review 2. Initial report thirty (30) days prior to PDR 3. Final report thirty (30) days prior to CDR	1. Review 2. Review 3. Approval
MA-26	4.8	Limited-Life Items List	1. Thirty (30) days prior to PDR 2. Updates to the Project Office within thirty (30) days of changes	Approval
MA-27	5.2	Software Assurance Plan	1. Preliminary plan to the Project Office thirty (30) days prior to SRR 2. Baseline plan to the Project Office fifteen (15) days prior to PDR 3. Updates to the Project Office fifteen (30) days prior to implementation	Information
MA-28	5.5	Software Assurance Status Report	1. Monthly beginning sixty (60) days after contract award	Information
MA-29	7.1	Risk Management Plan	Sixty (60) days after contract award	Approval
MA-30	7.2	Risk List	Monthly beginning with PDR	Review
MA-31	8.1	Systems Review Materials	1. Agenda fourteen (14) days prior to commencement of the review 2. Presentation materials seven (7) days prior to the review 3. Reference materials at the review	Information
MA-32	8.1	Action Item Responses	Thirty (30) days after end of review	Approval
MA-33	8.2	Peer Review Program	Sixty (60) days after contract award	Review
MA-34	9.1	System Performance Verification Plan	1. Preliminary plan thirty (30) days prior to PDR 2. Final plan thirty (30) days prior to CDR	1. Review 2. Approval
MA-35	9.2	Integration, Test, and Verification Plan	1. Preliminary plan thirty (30) days prior to PDR 2. Final plan thirty (30) days prior to CDR	1. Review 2. Approval
MA-36	9.3	System Performance Verification Matrix	Updated matrix included in the data packages for the Integrated Independent Reviews beginning with PDR	Review

DID #	MAR Paragraph	Title	Due	Purpose
MA-37	9.4	Integration, Test, and Verification Matrix	Updated matrix included in the review data package for milestone reviews beginning with PDR.	Review
MA-38	9.5	Verification Reports	1. Preliminary verification report within seventy-two (72) hours of test completion 2. Final verification report within thirty (30) days of test completion 3. Updated reports with the review data package at milestone reviews, beginning with CDR 4. Final report within thirty (30) days after completion of on-orbit checkout	Information
MA-39	10.3	ESD Control Plan	Thirty (30) days prior to PDR	Review
MA-40	11.1	Parts Control Plan	Thirty (30) days after contract award	Approval
MA-41	11.2	Parts Control Board	Thirty (30) days after contract award	Approval
MA-42	11.3.1	Parts Identification List	Ten (10) business days prior to the PCB meeting	Approval
MA-43	11.3.2	Project approved Parts List	Ten (10) business days prior to the PCB meeting at which they will be presented	Approval
MA-44	11.3.3	As designed Parts List	Ten (10) business days prior to the PCB meeting at which they will be presented	Approval
MA-45	11.3.4	As Built Parts List	Ten (10) business days prior to the PCB meeting at which they will be reviewed	Review
MA-46	12.1	Materials & Processes Selection, Control, and Implementation Plan	Sixty (60) days after contract award	Approval
MA-47	12.2	Life Test Plan for Lubricated Mechanisms	1. Plan thirty (30) days prior to PDR 2. Report thirty (30) days after acceptance test completion	1. Approval 2. Review
MA-48	12.3	Materials Usage Agreement	1. New MUAs thirty (30) days prior to CDR 2. Revised MUAs within thirty (30) days of identification	1. Approval 2. Approval
MA-49	12.4	Materials Identification and Usage List	1. Thirty (30) days prior to PDR 2. Thirty (30) days prior to CDR 3. Updates to the Project Office within thirty (30) days of identification	1. Review 2. Approval 3. Review
MA-50	12.5	Nondestructive Evaluation Plan	1. Thirty (30) days prior to PDR 2. Thirty (30) days prior to CDR 3. Updates thirty (30) days after identification	1. Review 2. Approval 3. Approval
MA-51	12.6	Printed Wiring Boards Test Coupons	As soon as practicable	Approval

DID #	MAR Paragraph	Title	Due	Purpose
MA-52	13.1	Contamination Control Plan	1. Plan thirty (30) days before PDR 2. Plan thirty (30) days before the CDR 3. Final thermal vacuum bakeout results provided within thirty (30) of completion 4. Contamination certificate of compliance with End Item Acceptance Data Package	1. Review 2. Approval 3. Review 4. Review
MA-53	13.2	Foreign Object Debris Prevention and Control Plan	Thirty days prior to PDR	Review
MA-54	15.4	GIDEP Alert and NASA Advisory Dispositions	1. Provide disposition of existing Alerts to the Project Office within 30 days of identification of potential use or use of an EEE part or material for review. 2. Provide disposition of subsequent Alerts to the Project Office regarding EEE parts or materials already approved for use within 30 days for review.	Review
MA-55	15.4	Significant Parts, Materials, and Safety Problems	Within thirty (30) days	Review
MA-56	16	End Item Acceptance Data Package	Thirty (30) days prior to end item delivery	Approval

* Delete one of the two per the related tailoring in the narrative