ICE, CLOUD, and Land Elevation Satellite

(ICESat-2) Project

Mission Assurance Requirements (MAR) ICESat-2-SMA-REQ-0009

Revision C

Effective Date: February 18, 2011

Expiration Date: February 18, 2016

National Aeronautics and Space Administration

Goddard Space Flight Center

Greenbelt, Maryland

CM FOREWORD

This document is an Ice, Cloud, and Land Elevation (ICESat 2) Project signature-controlled document. Changes to this document require prior approval of the applicable Product Design Lead (PDL) or designee. Proposed changes shall be submitted in the ICESat-2 Management Information System (MIS) via a Configuration Controlled Request (CCR), along with supportive material justifying the proposed change.

In this document, a requirement is identified by "shall," a good practice by "should," permission by "may" or "can," expectation by "will," and descriptive material by "is."

Questions or comments concerning this document should be addressed to:

ICESat-2 Configuration Management Office
Mail Stop 425
Goddard Space Flight Center
Greenbelt, Maryland 20771

***** All Signatures are available on-line at: https:// /icesat-2mis.gsfc.nasa.gov *****

CHANGE RECORD PAGE

Document Version	Document Release Date	CCR Number	CCR Approval Date	Pages Affected	Description
Rev -	4/21/2010	0002	4/21/2010	All	Initial release of baseline.
Rev A	11/29/2010	0044	11/22/2010	Most	Updated to bring it in sync with current ICESat-2 mission objectives and ATLAS instrument requirements.
Rev B	12/13/2010	0048	12/10/2010	Most	Editorial changes to: 8.0 Systems Reviews (This requirement applies equally to spacecraft, instrument subsystem and GSFC developers) This should read "(This requirement applies equally to mission, spacecraft, instrument and ground data system)." And in the DIDs, I updated the name for GSFC-STD-1001 in DID 8-1 and DID 8-2 to "Criteria for Flight and Flight Support Systems Lifecycle Reviews."
Rev C	02/18/2011	0062	02/18/2011	Most	Updated document to include RSDO / SC vendors comments for RFO

TABLE OF CONTENTS

Chapter 1. Requirement Foundation & Scope

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

1.0 PURPOSE

The purpose of this Mission Assurance Requirements (MAR) document is to prescribe the applicable Safety and Mission Assurance (SMA) requirements for the Ice, Cloud, and Land Elevation Satellite *(ICESat-2)* Project and ICESAT-2 developers. These requirements are defined as —Class C (Reference NASA Procedural Requirement NPR 8705.4). The Goddard Space Flight Center (GSFC) is responsible for the management and implementation of the ICESAT-2 Program for NASA. GSFC in turn has designated the ICESAT-2 Project GSFC as the authoritative project organization responsible for ICESAT-2. The term "developer(s)", when referred to herein, is defined as the ICESAT-2 Mission Element Providers (i.e., spacecraft, ATLAS, MOCC, Etc.). Specific distinction is provided as necessary.

1.1 SCOPE

The scope of this MAR applies to each developer as stated herein for the development of space flight hardware and any ground support equipment (GSE) that interfaces with flight hardware, instrument or spacecraft. For subsystems, and subcontracted items, the ICESAT-2 Project and its developers shall ensure flow-down of applicable MAR requirements to suppliers as appropriate and establish a process to verify compliance. This may necessitate defining a tailored subset of the MAR requirements appropriate to the complexity or criticality of the item being procured.

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

1. All flight hardware, either designed/built/provided by the developer or furnished by GSFC, from project initiation through launch and mission operations.
2. The ground system and its support equipment that interfaces with flight equipment to the extent necessary to assure the functional and flight integrity of flight items, including health and safety.
3. All software critical for mission success.
4. Mechanical and electrical Ground Support Equipment (GSE) and associated software that directly interfaces with flight deliverable items.
5. The spacecraft developer shall document this program in a Mission Assurance Implementation Plan (MAIP) as defined in Data Item Description (DID) 1-1.
6. All instrument subsystem developers shall document this program in a Product Assurance Implementation Plan (PAIP) as defined in Data Item Description (DID) 1-1b.

Managers of the assurance activities shall have direct access to developer management independent of project management, with the functional freedom and authority to interact with

all other elements of the project. Issues requiring project management attention shall be addressed with the developer(s) through the Project Manager(s) and/or Contracting Officer Technical Representative(s) (COTR).

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

When hardware that was designed, fabricated, or flown on a previous project is considered to have demonstrated compliance with some or all of the requirements of this document such that certain tasks need not be repeated, the developer shall demonstrate how the hardware complies with these requirements. The developer shall submit substantiating documentation in accordance with Data Item Description (DID) 1-2.

1.3 CONTRACT DELIVERY REQUIREMENTS LIST

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

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

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

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

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 APPLICABLE DOCUMENTS

See Appendix D

1.6 ACRONYMS AND GLOSSARY

See Appendix A

Chapter 2. Quality Management System

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

2.0 GENERAL

The developer shall submit a quality manual or plan that explains how the requirements of this document will be met. This document must be submitted to GSFC for approval with the proposal. The developer shall have a quality management system (QMS) that is compliant with the minimum requirements of SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing. The developer's Quality Manual shall be provided in accordance with DID 2-1. The ATLAS Instrument development team shall submit a Product Assurance Implementation Plan (PAIP) (DID-11b) prior to the Instrument Systems Requirements Review.

2.1 CONTROL OF NONCONFORMING PRODUCT

The developer shall have a closed loop system for identifying and reporting nonconformances, ensuring that corrective action is implemented to prevent recurrence. An initial finding (anomaly report.(DID 2-4) shall be entered into the system. The developer will audit and test as applicable to verify adequacy of the corrective action implemented. The system shall include a nonconformance review process, which shall consist of a preliminary review and a Material Review Board (MRB). The government project Safety and Mission Assurance (SMA) representative shall sign off on all MRB activity relating to flight hardware or ground support equipment (GSE) that interfaces with flight hardware.

2.2 PRELIMINARY REVIEW

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

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

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

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

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

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

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

A major nonconformance is defined as a material nonconformance affecting form, fit, function, reliability, or safety affecting the Contract end-item. Minor nonconformances are all other nonconformances, and tend to be cosmetic in nature.

2.3 MATERIAL REVIEW BOARD

Nonconformances not dispositioned by preliminary review, normally critical and major nonconformances, shall be referred to the MRB for disposition. MRB dispositions shall include scrap, rework, return to supplier, repair by standard or non-standard repair procedures, use-as-is, or request for major waiver. (DID 2-3) The MRB shall consist of a core team including QA, supplemented with other disciplines brought in as necessary. It shall be chaired by a developer representative responsible for ensuring that MRB actions are performed in compliance with this standard and implemented per developer procedures. This is usually a systems engineering function. Government participation and voting in MRBs will be for major non-conformances.

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

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

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

The Contractor shall provide notification to the Government of major nonconformances as soon as they are determined. It is intended that the Government will respond to proposed dispositions within 12 hours under normal circumstances. The Contractor shall notify the Government per the Government provided contact list. If no response is received within 12 hours, the Contractor may proceed per MRB direction. The Contractor shall inform the Government of MRB actions

2.4 REPORTING OF FAILURES

Reporting of failures shall begin as early in the life cycle as possible. Reporting must begin by the first power application at the start of end item acceptance testing, software anomalies beginning with first use of the flight build software or the first operation of a mechanical item. It shall continue through formal acceptance by the GSFC Project Office. Failures shall be reported to GSFC within 24 hours in accordance with DID 2-2.

Developer review/disposition/approval of failure reports shall be described in applicable procedure(s) included or referenced in the Quality Manual.

2.5 INSPECTION AND TESTING CONTROL

The developer shall establish and maintain documented procedures for inspection and testing activities in order to verify that the specified requirements for the product are met. The required inspection and testing, and the records to be established, shall be detailed in the product implement plans or documented procedures.

2.6 INSPECTION AND TEST STATUS CONTROL

The inspection and test status of product shall be identified by suitable means, which indicate the conformance or nonconformance of product with regard to inspection and tests performed. The identification of inspection and test status shall be maintained, as defined in the quality plan and/or documented procedures, throughout production, installation, and servicing of the product to ensure that only product that has passed the required inspections and tests is dispatched, used, or installed.

2.7 CONTROL OF MONITORING AND MEASURING DEVICES

The developer shall have a documented system for control of calibration and recall of test and measurement instrumentation.

Testing and calibration laboratories shall be compliant with the requirements of ANSI/NCSL Z540.3-2006 Requirements for the Calibration and Measuring of Test Equipment.

2.8 CONTROL OF CUSTOMER-SUPPLIED PRODUCT

The developer shall establish and maintain documented procedures for the control of verification, storage, and maintenance of customer-supplied product provided for incorporation into the supplies or for related activities. Any such product that is lost, damaged, or is otherwise unsuitable for use shall be recorded and reported to the customer.

2.9 PRODUCT IDENTIFICATION AND TRACEABILITY

The developer shall establish and maintain documented procedures for identifying the product by suitable means from receipt and during all stages of production, delivery, and installation.

Where and to the extent that traceability is a specified requirement, the developer shall establish and maintain documented procedures for unique identification of individual product or batches. This identification shall be recorded.

2.10 HANDLING, STORAGE, PACKAGING, PRESERVATION, & DELIVERY

The developer shall establish and maintain documented procedures for handling, storage, packaging, preservation, and delivery of product. The developer shall provide methods of handling product that prevent damage or deterioration. The developer shall use designated storage areas or stock rooms to prevent damage or deterioration of product, pending use or

delivery. The developer shall control packing, packaging, and marking processes to the extent necessary to ensure conformance to specified requirements. The developer shall apply appropriate methods for preservation and segregation of product when the product is under the developer's control. The developer shall arrange for the protection of the quality of product after final inspection and test. Where contractually specified, this protection shall be extended to include delivery to destination.

2.11 NEW ON-ORBIT DESIGN

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

2.12 FLOW-DOWN

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

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

The developer shall prepare and update as necessary a requirements verification matrix showing how the requirements are met by all suppliers.

2.13 PHOTOGRAPHIC DOCUMENTATION

The developer shall provide photographic documentation of all flight printed wiring assemblies, subsystem and system level boxes and structures, wiring harness routing and procured flight articles. These photographs shall accompany the hardware along with the data package to the next higher level of assembly through integration and testing. All such documentation is deliverable to the ICESat-2 project office at GSFC.

2.14 SURVEILLANCE

The work activities, operations, and documentation performed by the developer or his suppliers shall be subject to evaluation, review, audit, and inspection by government-designated representatives from the ICESAT-2 Project, the Government Inspection Agency, or an independent assurance contractor. The evaluation shall be consistent with the allowance to make maximum use of existing practices and procedures and/or meeting the intent of the ICESAT-2 MAR. If practical, the ICESAT-2 Project shall delegate in-plant responsibilities and authority to specifically designated organizations or representatives via a letter of delegation or letter of assignment, as agreed to in the product specific surveillance plan.

The developers of software and hardware 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.

For the spacecraft developer, the surveillance plan is specified in Spacecraft and Observatory Surveillance Plan, document # ICESat-2-SCSMA-PLAN-0193. For instrument subsystems-laser, the surveillance plan is defined in ICESat-2-ATSMA-PLAN-0070. For operations at GSFC, the instrument development team can expect oversight similar to that defined in the ICESat-2-ATSMA-PLAN-0070.

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.

Chapter 3. Safety, Reliability, & Mission Assurance Requirements

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

3.0 SYSTEM SAFETY

3.1 GENERAL

The developer shall implement a system safety program and support the ELV Safety Review Process as defined in paragraphs 2.4 & 2.5 of NPR 8715.7 Expendable Launch Vehicle Payload Safety Program, as well as meet launch service provider requirements, and launch 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 vehicle during the mission.
- 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

- AFSPCMAN 91-710, "Range Safety User Requirements"
- Attachment 1 to U.S. Air Force Range Safety Memorandum, "Joint 45 SW/SE and 30 SW/SE Interim Policy Regarding EWR 127-1 Requirements For System Safety for Flight and Aerospace Ground Equipment Lithium-Ion Batteries", dated May 4th, 2005.
- 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 (e.g. Astrotech)

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 3-1).

3.3.2 SAFETY REQUIREMENTS COMPLIANCE CHECKLIST

The developer shall prepare a Safety Requirements Compliance Checklist to demonstrate that the payload is in compliance with NASA and range safety requirements (DID 3-2). Noncompliances to safety requirements will be documented in waivers and submitted for approval.

3.3.3 HAZARD ANALYSES

3.3.4 PRELIMINARY HAZARD ANALYSIS –

The developer shall document Preliminary Hazard Analyses (PHA) (DID 3-3) to obtain an initial risk assessment and identify safety critical areas of a concept or system.

3.3.5 OPERATIONS HAZARD ANALYSIS

The developer shall perform and document an Operations Hazard Analysis (OHA) and a Hazard Verification Tracking Log 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 3-4). The developer shall maintain and update the Hazard Tracking Log during I&T activities to track open issues.

3.4 LIFTING DEVICE SAFETY REQUIREMENTS

The developer shall meet the safety requirements of NASA-STD-8719.9 Standard for Lifting Devices and Equipment when NASA-owned or NASA contractor-supplied equipment is used in support of NASA operations at NASA installations.

The developer shall meet the following safety requirements on lifting devices and equipment when performing NASA work at contractor facilities:

- The developer shall perform and document a recognized safety hazard analysis, such as fault tree analysis, FMEA, Operating and Support Hazard Analysis (O&SHA), on all lifting devices and equipment that will be used for critical lifts per NASA Standard 8719.9. (DID 3-5)
    - Determination of critical lifts shall comply with Paragraph 1.5.1 of NASA-STD-8719.9
- All cranes used for critical lifts shall have dual brakes and dual upper limit switches installed as defined by NASA Standard 8719.9.
- For Non-critical lifts, the developer shall comply with applicable ANSI/ASME B30 and B56 standards.
- The developer shall comply with applicable ANSI/ASME lifting device standards (e.g., B30, B56, etc.) for medical examinations.
- The developer shall ensure that all lifting device and equipment operators and riggers must be trained by a NCCCO (National Commission for the Certification of Crane Operators) certified (or equivalent) vendor.
    - If an in house training program is provided, the developer shall provide documentation notating a qualified employee that performs such training.
    - The contractor shall provide documentation that the vendor and/or house employee is qualified.

- For Non-critical lifts, the developer shall follow ANSI/ASME requirements for Daily (before use), Frequent (monthly) and Annual inspections
- For Critical lifts, the developer shall follow applicable NASA-STD-8719.9 paragraphs for Daily, Frequent and Annual inspections (i.e., 4.4, 5.4, etc.)
- Non destructive test (NDT) shall be performed for critical lift lifting devices (Frequent and Annual)
    - NDT Inspections shall be performed by an American Society of Nondestructive Testing (ASNT) or equivalent trained inspector

3.4.1 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 3-6).

3.4.2 INSTRUMENT SAFETY ASSESSMENT REPORT –

The developer shall generate an instrument safety assessment report (ISAR) to document the comprehensive evaluation of the risk being assumed prior to the testing or operation of an instrument. The spacecraft developer will use the ISAR as an input to the Safety Data Package (SDP). (DID 3-7)

3.4.3 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 3-7).

3.4.4 VERIFICATION TRACKING LOG

The developer shall prepare, implement, and maintain a Verification Tracking Log (VTL) (DID 3-8).

3.4.5 HAZARDOUS PROCEDURES FOR PAYLOAD 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 3-9). The developer shall provide safety support for hazardous operations at the launch site.

3.4.6 SAFETY WAIVERS

The developer shall submit Safety Waivers for variations from the applicable safety requirements in accordance with NPR 8715.7, paragraph 1.5 (DID 3-10).

3.4.7 INPUTS TO ORBITAL DEBRIS ASSESSMENTS

The developer shall provide inputs necessary to support the development of an Orbital Debris Assessment Report (ODAR) and an End of Mission Plan (EOMP) per the content defined in NASA-STD 8719.14, (DID 3-11).

3.4.8 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 per NPR 8621.1 NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping (DID 3-12). All accidents, test failures, or other mishaps or close calls shall be promptly investigated to determine the dominant root cause.

3.4.9 RANGE SAFETY FORMS

The developer shall prepare the following:

- Material Selection List for Plastic Films, Foams, and Adhesive Tapes (DID 3-13)
- Radiation forms/analysis (DID 3-14)
- Process Waste Questionnaire (DID 3-15)
- Environmental Impact Statement (DID 3-16)

Chapter 4. RELIABILITY

4.0 RISK ASSESSMENT AND RELIABILITY PROGRAM PLAN

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

The Developer shall prepare and implement a "PRA and Reliability Program Plan" using both qualitative and quantitative techniques to support decisions regarding mission success and safety throughout system development. The developer shall present the implementation of these plans and related activities at milestone reviews beginning with the System Requirements Review (DID 4-1). The ICESat-2 Reliability Program Plan (**ICESat-2-SMA-PLAN-0593**) describes the overall project plan and describes how the instrument & spacecraft activities are co-ordinated.

4.1 ANALYSES & DELIVERABLES

4.1.1 PROBABLISTIC RISK ASSESSMENT (PRA)

The Developer shall support the Project Team's effort to perform a simplified PRA (DID 4-2), by identifying major mission risk contributors as well as safety risks. The Developer shall provide needed information (DID 4-3) in the form of heritage information (*e.g.*, current flight history, current operating hours, operational and storage environments, TRLs); product information (*e.g.*, hardware and / or software configurations, parts lists, schematics); interim analysis (*e.g.*, working-level copies of fault tree analysis, failure mode, effects and criticality analysis, quantitative reliability block diagrams, reliability predictions); and / or process information (*e.g.*, design documents, manufacturing documents, parts program documents).

4.1.2 FAILURE MODES AND EFFECTS ANALYSIS (FMEA) AND CRITICAL ITEMS LIST (CIL)

The developer shall perform a FMEA and prepare and maintain a CIL for severity categories 1, 1R, 1S, 2, and 2R per Table 4.1 (DID 4-3) to the black box (or circuit block diagram) level. The developer shall analyze single point failure modes resulting in severity categories 1, 1R, 1S, 2, 2R, or 2S to determine the root cause, corresponding mitigation actions, and retention rationale. The developer shall address flight hardware and software that is designed, built, or provided by their organization or subcontractors, from project initiation through launch and mission operations. The developer shall address the ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items. The developer shall identify and address safety critical software, as defined in NASA-STD-8719.13.

Table 4.1 Severity Categories

Category	Severity	Description
1	Catastrophic	Failure modes that could result in loss of life, or permanently disabling or injuring of personnel, (flight or ground), and/or complete loss of flight or ground systems.
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	Critical	Failure modes that could result in loss of one or more mission objectives as defined by the GSFC project or causes severe injury or occupational illness.
2R		Failure modes of identical or equivalent redundant hardware or software that could result in Category 2 effects if all failed.
2S		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 2 consequences.
3	Significant	Failure modes that could cause degradation to mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

4.2 FAULT TREE ANALYSIS

The Developer shall perform qualitative fault tree analyses: (1) to address mission failures to operations and/or disposal and degraded modes of operation relative to their mission element, and (2) to address undesirable fault propagation scenarios as part of supporting PRA efforts (DID 4-5). The Developer shall identify and address safety critical software as defined in NASA-STD-8719.13 that is identified as part of the FMECA process.

4.3 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 (DID 4-5).

4.4 WORST CASE ANALYSIS

WCA is not required because ICESat-2 is a class C mission, but the Project Team may specifically request it from the Developer at a later time. If requested, this work will be considered additional scope.

4.5 RELIABILITY ASSESSMENTS AND PREDICTIONS

The developer shall perform comparative numerical reliability assessments and reliability predictions (DID 4-7) to support FMEA/CIL, PRA, trades, and design efforts as requested.

4.6 RELIABILITY ANALYSIS OF TEST DATA

The developer shall use data from the test program to assess reliability and identify potential or existing problem areas.

4.7 ANALYSIS OF TEST RESULTS

The developer shall document the analysis of test information, trend data, and failure investigations with respect to reliability and report the results as defined in the approved PRA and Reliability Program Plan.

4.8 LIMITED LIFE ITEMS

The developer shall prepare and implement a plan to identify and manage limited life items (DID 4-8).

Chapter 5. SOFTWARE ASSURANCE (FLIGHT AND GROUND SEGMENTS)

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

5.0 APPLICABLE 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 complex electronics that include microprocessors.

Software is **safety critical** if the software can cause or contribute to a catastrophic or critical hazard to humans, flight hardware or facilities,provides an inhibit(s) that is necessary to meet the dual or single failure tolerance requirement associated with such a hazard (ref. section 3.1), or provides functionality (e.g., Guidance, Navigation and Control capability during controlled re-entry) that is necessary to meet the NASA requirements for post mission orbital debris control and end of mission planning in NASA-STD-8719.14, "Process for Limiting Orbital Debris". The identification of safety critical software is driven by the Preliminary Hazard Analysis, Orbital Debris Assessment Report, End of Mission Plan, and system/component level analyses, including Fault Tree Analysis (FTA), and Failure Modes Effects and Analysis (FMEA). Safety critical software is focused on hazards specific to Integration and Test, through launch, and up through spacecraft separation from the launch vehicle, and where applicable re-entry/recovery.

Software is **mission critical** if the software can cause, contribute to, or mitigate the loss of capabilities that are essential to achieving the mission objectives. The identification of mission critical software is driven by the flow-down of mission objectives, and system/component level reliability analyses, including Fault Tree Analysis (FTA), and Failure Modes Effects and Analysis (FMEA). Mission critical software is focused on failure modes specific to all project lifecycles and mission phases.

The Contractor shall comply with the following for software and firmware, hereafter collectively referred to as software:

a. NPR 7150.2A, NASA Software Engineering Requirements;

b. NASA-STD-8719.13, Software Safety Standard; and
c. NASA-STD-8739.8, NASA Standard for Software Assurance.

5.1 SOFTWARE ASSURANCE PROGRAM

The developer shall prepare and implement a software assurance plan for software, as defined in section 5.1 (DID 5-1), that complies with:

- NASA-STD-8739.8, NASA Standard for Software Assurance
- NASA-STD-8719.13, Software Safety Standard
- NPR 7150. 2, the NASA Software Engineering Requirements (see the SOW and associated deliverables for software engineering)

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

The developer shall document the software assurance program in a Software Assurance Plan (DID 5-2). The plan shall 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 shall include the software assurance processes, procedures, tools, and techniques to be used commensurate with the Software Classification Assessment. The plan shall address the necessary collaboration between software assurance, system safety, system reliability, and software engineering.

When Independent Verification and Validation (IV&V) is performed, the developer shall coordinate with IV&V personnel to share information and address approved corrective actions.

When performing assurance related activities on digital Complex Programmable Logic Devices (i.e., FPGAs, ASICs, etc.) that include microprocessors, software assurance practitioners shall develop a methodology consistent with NPR 7150.2A, to evaluate/establish the following:

- Design & Test Controls;
- Version Control;
- Configuration Management Control
- Load Verification Facilitating Performance/ Safety/Reliability Analyses;

5.2 SOFTWARE SAFETY ANALYSES

Based on top level events obtained from the PHA (DID 3-4),) and the ODAR (DID 3-11), the developer shall perform Fault Tree Analysis (FTA) to identify software that is safety critical, as defined in section 5.0. 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, including loss of public life as a result of failures during controlled re-entry (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.

For critical software, as identified by the FTA, the developer shall produce a functional block diagram (FBD) that accounts for the interfaces, corresponding inputs/outputs, and the sequence of operations between the software and other components of critical system, subsystem, or task-level level functions. The results of the Software Safety Analyses, including references to the associated software and fault management requirements, are to be incorporated into all applicable hazard reports and delivered as part of the SDP (DID 3-8)) and/or provided as inputs to the project office for incorporation into the ODAR and EOMP, if applicable (DID 3-11)._.

5.3 SOFTWARE RELIABILITY ANALYSES

The developer shall include in its software plans, the processes and procedures for identifying mission critical software, and performing the required reliability analyses. The developer's software plans shall include details on the following processes:

- Integrating software into the system level reliability analysis
- Conducting and reviewing software subsystem and component/task level FTAs and FMEAs.
- Deriving fault and failure management requirements from software subsystem and component/task level FTA and FMEAs.
- Reviewing and verifying fault and failure management requirements.

Effective software reliability is a collaborative effort, involving software engineering, systems engineering, reliability engineering, and software assurance. As such, the software reliability analyses shall be subject to the specifications of the related reliability engineering DIDs, and included in the submission of reliability engineering CDRLs. The details of the collaboration between engineering disciplines shall be captured in the associated plans, including the Reliability Program Plan (DID 4-1), Software Assurance Plan (DID 5-1), Systems Engineering Plan, and SW Development plans.

The developer shall perform Fault Tree Analysis (FTA) to identify software that is mission critical, as defined in section 5.0. For mission critical software, the FTA shall be derived from

top-level events associated with Loss of Mission Scenarios. The developer shall iterate its Software Reliability Analyses as the system requirements and design specifications evolve.

For critical software, as identified by the FTA, the developer shall produce a functional block diagram (FBD) that accounts for the interfaces, corresponding inputs/outputs, and the sequence of operations between the software and other components of critical system, subsystem, or task-level level functions.

The developer shall utilize the FBD(s) as input into the Failure Mode Effects and Analysis (FMEA) of critical software (DID 4-3). The developer shall update requirement specifications associated with critical software, to uniquely identify the associated requirements, and capture fault and failure management requirements derived from the FMEA of critical software. This provides necessary traceability between the software reliability analyses, and the fault management design.

For details concerning the reliability engineering tasks that will govern the assessment of safety and mission critical software, see MAR Section 4, PROBABILITY RISK ANALYSIS AND RELIABILITY, and Section 3, SYSTEM SAFETY.

5.4 REVIEWS

In addition to the reviews specified in Section 8, the developer shall conduct and provide advance notification to the project office of the following reviews:

- Software Peer Reviews (as specified by NPR 7150.2A)
- Software Test Readiness Review
- Software Acceptance Review
- System level safety reviews

5.5 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; r requirements specifications, design documents, test plans, test cases, test procedures, test results, schedule, maintenance plans)
- Electronic access to the software review results
- Schedule of assurance reviews, audits, and assessments of the developer's processes and products
- Access to the corrective actions from process and product audits
- Notification of and government participation in engineering peer reviews (e.g., code reviews, test plan/procedure reviews)
- Access to review action item status and resolution
- Access to monthly Software Measurement/Metrics data
- Access to requirements traceability matrices and data
- Software Assurance Status Report (DID 5 2)

5.6 GOVERNMENT FURNISHED EQUIPMENT (GFE), EXISTING, AND PURCHASED SOFTWARE

The developer shall ensure that software provided as GFE, existing, and purchased meets the functional, performance, and interface requirements. The developer shall ensure that the software meets applicable standards, including those for design, code, and documentation.

Chapter 6. Ground Data Systems Assurance Requirements

(This requirement applies only to the contractor providing ground support data systems services)

6.0 GENERAL

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

6.1 QUALITY MANAGEMENT SYSTEM

QMS-related requirements are discussed in Section 2 of this document. It should be noted that the QMS shall be applied to the development and assurance functions for GDS components as well. In all cases, the development effort shall provide evidence (records for GSFC review) as insight to the quality of the developing software, hardware and other GDS components as evidence of application of QMS processes, and as status of assurance problems, safety issues and organizational/personnel changes. The developer shall provide GSFC with a GDS MAIP. (DID6-1). Records shall include any corrective actions, relating to GDS development, recommended by QMS audits. The developer will allow NASA audits, when deemed necessary by the Project Manager, to assure compliance of the developer's QMS with SAE AS9100 Quality Systems - Aerospace and to assure that the QMS is applied to the contracted activities.

The developer shall provide GSFC with a Mission Operations Center Equipment Plan (DID 6-2) that documents the developer's plans for developing, building, and maintaining ground operations equipment to support launch and flight operations.

6.2 REQUIREMENTS

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

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

The developer shall baseline the GDS requirements early in the development effort, specifically in conjunction with a formal requirement review. The developer shall maintain the GDS requirements under configuration control throughout the project life cycle. All changes to the

GDS requirements, including those generated both internally and externally shall be managed by the developer's CCB process and reviewed/approved as applicable by GSFC.

6.3 REVIEWS

Formal reviews are discussed in Section 8 of this document.

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

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

6.4 ASSURANCE ACTIVITIES

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

Requirements Phase

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

- Analyze and refine the requirements to assure they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information.

- Ensure requirements are generated, analyzed, refined, decomposed and allocated to appropriate GDS components through the use of a systems analysis and allocation process. This process shall be used to verify requirements are correct and complete at each level prior to further allocation and decomposition, and to verify them for feasibility and top-level design concept prior to further allocation.

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

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

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

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

- Generate, document and maintain a requirements verification matrix.

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

6.4.1 DESIGN PHASE

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

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

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

- Conduct design walkthroughs and reviews.

- Place design under CM

6.4.2 IMPLEMENTATION PHASE

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

- Define and document the components of each build, delivery and/or release.
- Conduct peer reviews/walkthroughs for code.
- Conduct unit testing.
- Conduct reviews and appropriate tests at the end of this development process phase, to ensure that the requirements have been correctly implemented into design, code, documentation and data.
- Allocate and maintain traceability between the GDS architecture/components and the GDS requirements.

6.4.3 TESTING PHASE

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

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

- Generate test procedures that implement the test plans and facilitate the verification and validation of GDS requirements. All test procedures shall be made subject to GSFC review and approval as applicable.
- Maintain a process to ensure that any test tools and test data are qualified prior to use during testing activities.
- Ensure that test personnel attend and participate as necessary in various reviews throughout the life cycle, to include but not limited to requirements, architecture and design reviews.
- Identify and document test readiness criteria for both formal and informal testing activities. Test criteria shall be made subject to GSFC review and approval as applicable.
- Maintain and update the RVM generated earlier in the life cycle to include the status (pass, fail, deferred, etc.) of each requirement throughout the testing phases and various testing activities.
- Test reports should document the validation of requirements, specific tests completed, conformance of the test results to the expected results, the number, type and criticality of any identified discrepancies/nonconformances, identification of the hardware, software and other GDS components tested including version number, etc.
- Document all defects/nonconformances encountered during the testing activities. These defects/nonconformances shall be assessed for criticality, severity, impact, etc. to determine appropriate action and resolution. The developer shall track and report on the status of all defects/nonconformances.
- Identify all nonconformances that impact the developer's ability to meet GDS requirements and document these items in a waiver, which must be reviewed/approved by GSFC as applicable.
- Ensure an independent entity, either internal or external QA representatives/personnel, witness the final (launch ready release) testing activities for Class B safety critical SW.
- Ensure and maintain configuration control of the test environment including hardware, software, simulators, test data, databases and other components throughout the test program.
- Assess all changes made to the system architecture and its components to determine the necessity for regression testing. The developer shall conduct regression testing based upon assessed and approved/implemented changes as appropriate.
- Conduct contingency and off-nominal condition testing.

- Conduct pre-test briefings and generate briefing messages where appropriate to facilitate the coordination of various test related activities. Briefing message contents may include, but are not limited to:
  - Test Case/Procedure Name/Number.
  - Purpose of the Test.
  - Testing Dates/Times.
  - Test Participants and required resources (scheduling of lab and station support, data sources (e.g. SC, SC data tape, engineering test unit or SC simulator), software, hardware and support system configurations (to include release/version numbers where appropriate).
  - GDS requirements to be verified.
  - Contact list to include names and numbers of test participants.
- Conduct post-pass and post-test debriefings. During these debriefs, the developer shall summarize test results, disposition the test (pass/fail, etc), deviations from test procedures, requirements verified and discrepancy reports generated, etc.
- Conduct mission simulations to validate nominal and contingency mission operating procedures and to provide for operator familiarization training. In order to provide ample time for checkout of operational configurations, it is considered essential that users participate in mission simulations.

6.4.4 DELIVERY PHASE

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

- System delivery letter:
  - Description of hardware and software delivery contents.
  - Build instructions, including the source code, databases and all files required to complete a successful software build.
  - Special operating instructions.
  - List and copy of resolved anomaly reports and change requests.
  - List and copy of unresolved anomaly reports and change requests.

- Matrix of requirements addressed by this release, including waivers for those requirements not met as appropriate.
- List of changes to documentation associated with this release.
- Verification success criteria.
- Known problems and workarounds.

- Software delivery media.
- Accompanying documentation.

6.5 GFE, COTS, EXISTING AND PURCHASED SOFTWARE

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

6.5.1 COTS MANAGEMENT

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

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

6.6 DATABASES

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

6.7 SECURITY ASSURANCE

- The developer shall conduct a security program to identify and mitigate security risks associated with the GDS and its components. All security risks shall be assessed/analyzed for impact and likelihood of occurrence.

- The security program shall ensure that security requirements are established, documented and implemented during all phases of the software life cycle. Security tasks and activities shall include the addressing of security concerns during reviews, analyses, inspections, testing and audits.

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

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

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

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

6.8 ELECTROMAGNETIC COMPATIBILITY CONTROL

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

6.9 RELIABILITY AND AVAILABILITY

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

- Starting in the conceptual design stage the developer shall clearly define, based upon ICESAT-2 mission success criteria and reliability requirements, levels of performance. The developer shall establish and implement specific design criteria needed to mitigate unacceptable levels of performance. Design criteria shall be accessible for GSFC review.

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

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

  - Time required to remove and replace the defective LRU.

- Time required to complete checkout and restore operational status.

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

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

6.10 SYSTEM SAFETY

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

Chapter 7. Risk Management Requirements

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers- the degree of applicability is limited to the level of what is being procured under contract)

7.0 GENERAL

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

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

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

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

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

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

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

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

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

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

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

7.1 APPLICABLE DOCUMENTS

GPR 1060.2 Management Review and Reporting for Programs and Projects

GPR 8700.4	Integrated Independent Reviews
NPR 5100.4	Federal Acquisition Regulation Supplement
NPR 7120.5	Program and Project Management Processes and Requirements
NPR 8000.4	Risk Management Procedural Requirements
NPR 8715.3	NASA Safety Manual

7.2 RISK MANAGEMENT PLAN

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

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

7.3 RISK LIST

The developer shall maintain a Risk List (DID 7-2) throughout the project life cycle, along with programmatic impacts. The list should indicate which risks have the highest probability, which have the highest consequences, and which risks represent the greatest risk to mission success. The list should also identify actions being taken to address each specific risk. The Risk List shall be configuration controlled.

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

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

- Description of the risk, including primary causes and contributors, current mitigation strategy, and information collected for tracking purposes.
- Primary consequences should the undesired event occur.

- Estimate of the probability of occurrence (qualitative or quantitative) together with the uncertainty of the estimate and the effectiveness of any implemented risk mitigation measures.
- Potential additional risk mitigation measures, which shall include a comparison of the cost of risk mitigation versus the cost of occurrence multiplied by the probability of occurrence.
- Characterization of a primary risk as "acceptable" shall be supported by a rationale (with the concurrence of the GPMC) that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

Chapter 8. SYSTEMS REVIEWS

8.0 SYSTEMS REVIEWS

(This requirement applies equally to mission, spacecraft, instrument and ground data system)

The developer shall participate in the implementation of the Integrated Independent Review Program as required by the ICESat-2 Systems Review Plan, ICESat2-MGMT-PLAN-0085.

The developer shall provide a review agenda, presentation materials, and a copy of reference materials at the reviews (DID 8-1).

The developer shall submit responses to review action items (DID 8-2).

8.1 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 8-3) consistent with the ICESat-2 Systems Review Plan, ICESat2-MGMT-PLAN-0085

Chapter 9. SYSTEM PERFORMANCE VERIFICATION

9.0 SYSTEM PERFORMANCE VERIFICATION PROGRAM PLAN

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

The developer shall plan and implement a system performance verification program per the requirements of GSFC-STD-7000 General Environmental Verification Standard (DID 9-1) and as tailored by product specific Environmental Description Documents.

9.1 ENVIRONMENTAL VERIFICATION PLAN

The developer shall prepare and implement an environmental verification plan (DID 9-2).

9.2 SYSTEM PERFORMANCE VERIFICATION MATRIX

The developer shall prepare and maintain a system performance verification matrix (DID 9-3).

9.3 ENVIRONMENTAL TEST MATRIX

The developer shall prepare and maintain an environmental test matrix (DID 9-4).

9.4 VERIFICATION REPORTS

The developer shall prepare and submit verification reports (DID 9-5).

9.5 SYSTEM PERFORMANCE VERIFICATION REPORT

The developer shall prepare and submit system performance reports (DID 9-6).

Chapter 10. CONTROL PRACTICES

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

10.0 WORKMANSHIP

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-8739.2 Surface Mount Technology
- NASA-STD-8739.3 Soldered Electrical Connections
- NASA-STD-8739.4 Crimping, Interconnecting Cables, Harnesses, and Wiring
- NASA-STD-8739.5 Fiber Optic Terminations, Cable Assemblies, and Installation
- IPC-2221 Generic Standard on Printed Board Design
- IPC-2222 Sectional Design Standard for Rigid Organic Printed Boards
- IPC-2223 Sectional Design Standard for Flexible Printed Boards
- IPC-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)
- IPC-6012B 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
- 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)

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

- MIL-HDBK-470, Designing and Developing Maintainable Products and Systems,

- MIL-STD-1540, Structural Design and Test Factors of Safety for Spaceflight Hardware ,
- NASA-STD-5017, Design and Development Requirements for Mechanisms,
- NASA-STD-5001, Structural Design and Test Factors of Safety for Spaceflight Hardware,
- NASA-HDBK-5016, Fracture Control Handbook for Spaceflight Composite Structures, and
- ANSI/AIAA S-080, Space Systems – Metallic Pressure Vessels, Pressurized Structures, and Pressure components.

10.1 DESIGN AND PROCESS QUALIFICATION

The developer shall qualify designs and processes that are not covered by the above standards.

10.2 ELECTROSTATIC DISCHARGE CONTROL (ESD)

The developer shall prepare and implement an ESD control program that conforms to the requirements of ANSI/ESD S20.20 (DID 10-1).

10.3 CONTAMINATION CONTROL

10.3.1 CONTAMINATION CONTROL PLAN

The developer shall prepare and implement a contamination control program (DID 10.2)

10.4 METROLOGY AND CALIBRATION

10.4.1 METROLOGY AND CALIBRATION PROGRAM

The developer shall plan and implement a documented metrology and calibration program. The developer shall comply with ANSI/NCSL Z540.3:2006 Calibration Laboratories and Measuring and Test Equipment – General Requirements.

10.4.2 USE OF NON-CALIBRATED INSTRUMENTS

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.

10.5 CIRCUIT BOARD TRACE CUTS, JUMPER WIRES, AND DEAD-BUG PARTS

The use of trace cuts, jumper wires, and dead-bug parts is prohibited for flight circuit boards, unless approved by Material Review Board.

10.6 USE OF SPLICES

The use of splices is prohibited unless approved by the Material Review Board.

Chapter 11. PARTS

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

11.0 GENERAL

The developer shall plan and implement a parts control program (PCP) per the Level 2 requirements of GSFC EEE-INST-002 (DID 11-1) that includes the handling of alerts and advisories as defined in Chapter 14.

11.1 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 11-2). The PCB membership shall include the Government Project Parts Engineer (PPE) as a voting member. The Government PPE (or a designated alternate) will be present at all PCB meetings.

11.2 EEE PARTS LISTS

The developer shall develop and maintain EEE parts lists.

11.3 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 11-3).

11.4 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 11-4).

11.5 AS-DESIGNED PARTS LIST (ADPL)

The developer shall prepare a list of EEE parts that are used in the design of flight hardware (DID 11-5).

11.6 AS-BUILT PARTS LIST (ABPL)

The developer shall prepare a list of EEE parts that are used in the flight hardware (DID 11-6).

11.7 DESTRUCTIVE PHYSICAL ANALYSIS (DPA)

A sample of each lot date code of hybrid microcircuits, microcircuits and semiconductor devices as noted below shall be subjected to a DPA unless a DPA was performed as part of the manufacturers screening program. DPA shall be performed in accordance with S-311-M-70. Variations to DPA sample size requirements for DPA procedure shall be determined and approved by PCB on a case by case basis. Additional DPAs may be required based on parts history and shall be determined on a case by case basis by the PCB.
Hybrid Microcircuits – all reliability levels
Microcircuits – Below MIL-PRF-38535 reliability level —Q||
Semiconductor diodes and transistors – Below —JANTXV||

11.8 BATTERY FOREIGN OBJECTS DEBRIS (FOD) PLAN

An FOD shall be developed in accordance with DID 11-7. The intent of this plan is to reduce short circuit events associated with FOD, which may result in loss of the battery.

The FOD mitigation plan should include the following:

- A description of how FOD is prevented from entering the cell or being generated in the cell (ie: cell assembly in a clean room, cleaning/training frequency, cleaning/brushing and/or inspection of plates/windings, handling of plates/windings, etc.)
- A description of how FOD is detected (ie: radiography such as CT scan, electrical characterization, sample cells DPA'ed, etc).
- A description of what steps are taken should a cell be suspected of having FOD or other reject cells (ie: radiography, electrical characterization, DPA, etc).
- A description of how these reports are shared and used within manufacturing and engineering to prevent future issues and to improve production.

Chapter 12. MATERIALS AND PROCESSES

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

12.0 GENERAL

The developer shall prepare and implement a materials and processes selection, implementation, and control plan per the requirements of NASA-STD-6016 (DID 12-1).

12.1 LIFE TEST PLAN FOR LUBRICATED MECHANISMS

The developer shall prepare and implement a life test plan for lubricated mechanisms (DID 12-2).

12.2 MATERIALS USAGE AGREEMENT (MUA)

The developer shall prepare materials usage agreements (DID 12-3).

12.3 MATERIALS IDENTIFICATION AND USAGE LIST (MIUL)

The developer shall prepare a materials identification and usage list (DID 12-4).

12.4 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 12-5).

12.5 PRINTED WIRING BOARD TEST COUPONS

The developer shall provide printed wiring board test coupons to the GSFC or to a GSFC approved facility for analysis (DID 12-6). The developer shall not use printed wiring boards until the analysis results are received.

12.6 LEAD-FREE AND TIN WHISKER CONTROL

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.

- GEIA –STD-0005-1: Performance Standard for Aerospace and High Performance Electronics Systems Containing Lead-free Solder
- GEIA-STD-0005-2: Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High Performance Electronic Systems

12.7 BROMINATED POLYIMIDE BOARD LAMINATE / DOCUMENTATION

Polyimide laminates shall contain no discrete bromide particles – the polyimide matrix of the laminate must be fully homogeneous to avoid potential for Conductive Anodic Filament (CAF) failures.
Laminate manufacturer, material reference number, and /IPC designation shall be included in project materials list. In addition, coupon submittal sheets shall clearly note if brominated material was used in the PWB fabrication.
Note: Polyimide without the bromine additive continues to remain a recommended material. Brominated polyimide materials with no optically discernible bromide particles are equally acceptable for use.

12.8 TITANIUM ALLOY TEST COUPONS

The developer shall provide third party strength verification of all titanium stock. Titanium Alloy test coupons, reports, and certification shall be retained by developer and made available to GSFC on request.

Chapter 13. Environmental

(This requirement applies to spacecraft developers)

The developer shall meet the requirements and guidelines for the environmental verification program for the Ice, Cloud, and Land Elevation Satellite-2 (ICESAT-2) observatory, instrument, spacecraft bus, subsystems and components found in the ICESat-2-SYS-REQ-0518, ICESat-2 Environmental Requirements Document.

13.0 RADIATION

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers when considering design of PWAs)

The developer shall prepare a radiation assessment covering applicable effects, including, but not limited to

- Spacecraft Charging (S/C)
- Total Ionizing Dose (TID)
- Displacement Damage
- Single Event Effects (SEEs):
  - Single event upset (soft error)
  - Single event latchup/functional interrupt (soft or hard error)
  - Single event burnout (hard failure)
  - Gate rupture (hard error/failure)

13.1 DISPOSAL/ORBITAL DEBRIS ASSESSMENT

The developer shall prepare an Orbital Debris Assessment (ODA) per NSS 1740.14/ NPD 8710.3B (DID 13-1).

13.2 NEPA/EA

The developer shall support the project team's efforts to comply with NPR 71250.5D & NPR 8580.1 that implement the National Environmental Policy Act and Executive Order 12114.

Chapter 14. GIDEP ALERTS AND PROBLEM ADVISORIES

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

14.0 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).

14.1 REVIEWS

The developer shall review the following, hereafter referred to collectively as Alerts, for affects on NASA products: GIDEP Alerts; GIDEP SAFE-ALERTS; GIDEP Problem Advisories; GIDEP Agency Action Notices; NASA Advisories and component issues as distributed by the project office.

14.2 ACTIONS

The developer shall recommend corrective action(s) to eliminate or mitigate the effects of Alerts on NASA products. Upon review of the recommended actions, the government will direct recommended or other action(s) to be taken to address the alert.

14.3 REPORTING

The developer shall report the results of Alert reviews and actions taken (DID 14-1).

The developer shall prepare and submit failure experience data 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.

The developer shall report significant EEE parts, materials, alert, and safety problems (DID 14-2).

Chapter 15. End Item data Package

The developer shall prepare, maintain, and submit an end item acceptance data package that documents the design, fabrication, assembly, test, and integration of the hardware and software being delivered and is included with the end item delivery and defined in the DID.(DID 15-1).

Chapter 16. Configuration Management Controls

(This requirement applies equally to spacecraft, instrument subsystem and GSFC developers)

16.0 DOCUMENT CONTROL

The developer shall participate in the implementation of the Configuration Control Plan as required by NPR 7123.1 and the ICESat-2 Configuration Management Procedures, ICESat2-0019.

16.1 APPENDIX A: ACRONYMS AND DEFINITIONS

I. ACRONYMS

ABPL	As-Built Parts List
ABML	As-Built Materials List
ANSI	American National Standards Institute
ASIC	Application Specific Integrated Circuits
ASQ	American Society for Quality
ASTM	American Society for Testing and Materials
BB	Ball Bearing
BGA	Ball Grid Array
BOL	Beginning of Life
CAGE	Commercial and Government Entity Code
CCB	Configuration Control Board
CCP	Contamination Control Plan
CDR	Critical Design Review
CIL	Critical Items List
CM	Configuration Management
CONR	Confirmation Review
COTR	Contracting Officer's Technical Representative
CPT	Comprehensive Performance Test
CVCM	Collected Volatile Condensable Mass
DID	Data Item Description
DoD	Department of Defense

DPA	Destructive Physical Analysis
EWR-127-1	Range Safety Requirement
EDU	Engineering Development Unit
EEE	Electrical, Electronic, and Electromechanical
ELV	Expendable Launch Vehicle
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharge
FMEA	Failure Modes and Effects Analysis
FOR	Flight Operations Review
FRB	Failure Review Board
FTA	Fault Tree Analysis
FRR	Flight Readiness Review
GEVS	General Environmental Verification Specification
GEVS-SE	General Environmental Verification Specification for STS & ELV Payloads, Subsystems, and Components
GFE	Government-Furnished Equipment
GFM	Government Furnished Material
GIDEP	Government Industry Data Exchange Program
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
I&T	Integration and Test
ISO	International Standards Organization
IV&V	Independent Verification and Validation
LRR	Launch Readiness Review
LWS	Living With a Star
MAE	Material Assurance Engineer
MAR	Mission Assurance Requirements
MCP	Multi-Chip Module
MIL	Materials Identification List

MOR	Mission Operations Review
MRB	Material Review Board
MRR	Mission Readiness Review
MSFC	Marshall Space Flight Center
MUA	Materials Usage Agreement
NAS	NASA Assurance Standard
NASA	National Aeronautics and Space Administration
NHB	NASA Handbook
NRCA	Nonconformance Reporting and Corrective Action
NSTS	National Space Transportation System
OSSMA	Office of Systems Safety and Mission Assurance
PAIP	Performance Assurance Implementation Plan
PAPL	Project Approved Parts List
PMPCB	Parts, Materials and Processes Control Board
PCP	Parts Control Plan
PDR	Preliminary Design Review
PER	Pre-Environmental Review
PHA	Preliminary Hazard Analysis
PIL	Parts Identification List
PIND	Particle Impact Noise Detection
PPL	Preferred Parts List
PRA	Probabilistic Risk Assessment
PSR	Pre-Shipment Review
PWB	Printed Wiring Board
QCM	Quartz Crystal Microbalance
QMS	Quality Management System
SAM	Systems Assurance Manager
SB	Sleeve Bearing
SCC	Stress Corrosion Cracking
SCM	Software Configuration Management

SCR	System Concept Review
SOW	Statement of Work
SQE	Software Quality Engineer
SQMS	Software Quality Management System
SMA	Safety and Mission Assurance
SRO	Systems Review Office
SRR	Software Requirements Review
STS	Space Transportation System (Shuttle)
TML	Total Mass Loss
TRR	Test Readiness Review
V&V	Verification and Validation

APPENDIX B: DEFINITIONS

The following definitions apply within the context of this document:

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

Anomaly: An anomaly is an unexpected event, hardware or software damage, a departure from established procedures or performance or a deviation of hardware or software performance outside certified design/performance specification limits. Anomalies include sense of problem and failure. This includes unexpected power glitches, single event upsets, unexpected degradation and autonomous resets.

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

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

Comprehensive Performance Test (CPT): The operation of a unit in accordance with a defined operational procedure to verify that performance is compliant with all parameters of the specified requirements. CPTs are performed at major project milestones and serve as a quality control screen to detect deficiencies, establish performance baselines, identify subtle changes, and provide accumulated data for trending analyses.

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

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

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

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

Critical: A potential failure effect which would result in a significant (as defined by the project) performance degradation of an item of hardware or a mission.

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

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

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

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

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

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

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

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

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

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

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

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

Level of Assembly: The environmental test program as defined by the GEVS-SE generally starts at the component or unit-level assembly and continued hardware/software build through the system level (referred to in GEVS-SE as the payload or spacecraft level). The assurance program includes the part level. Validation testing may also include testing at the assembly and

subassembly levels of assembly; for test record keeping these levels are combined into a "subassembly" level. The validation program continues through launch, and on-orbit performance. The following levels of assembly are used for describing test and analysis configurations:

a. Part: A hardware element that is not normally subject to further subdivision or disassembly without destruction of design use. Examples include resistor, integrated circuit, relay, connector, bolt, and gaskets.
b. Subassembly: A subdivision of an assembly. Examples are wire harness and loaded printed circuit boards.
c. Assembly: A functional subdivision of a component consisting of parts or subassemblies that perform functions necessary for the operation of the component as a whole. Examples are a power amplifier and gyroscope.
d. Component: A functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem's operation. Examples are electronic box, transmitter, gyro package, actuator, motor, and battery.
e. Section: A structurally integrated set of components and integrating hardware that form a subdivision of a subsystem, module, etc. A section forms a testable level of assembly, such as components/units mounted into a structural mounting tray or panel-like assembly, or components that are stacked.
f. Subsystem: A functional subdivision of a payload consisting of two or more components. Examples are structural, attitude control, electrical power, and communication subsystems. Also included as subsystems of the payload are the science instruments or experiments.
g. Instrument: A spacecraft subsystem consisting of sensors and associated hardware for making measurements or observations in space.
h. Module: A major subdivision of the payload that is viewed as a physical and functional entity for the purposes of analysis, manufacturing, testing, and record keeping. Examples include spacecraft bus, science payload, and upper stage vehicle.
i. Payload: An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space. For the purposes of this document, "payload" and "spacecraft" are used interchangeably. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.
j. Spacecraft: See Payload. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

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

Margin: The amount by which hardware capability exceeds mission requirements

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

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

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

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

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

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

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

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

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

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

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

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

Appendix C: Data Item Descriptions (DIDs)

DID 1-1A MISSION ASSURANCE IMPLEMENTATION PLAN

Title: Mission Assurance Implementation Plan	DID 1-1
Reference: ICESat-2 MAR Paragraph 1.1	
Use: Documents the developer's plan for implementing a system safety and mission assurance program	
Related Documents:	
Place/Time/Purpose of Delivery: - Delivered to the Project Office sixty (60) days after contract award for approval - Updates shall be delivered to the Project Office within thirty (30) days of plan changes including but not limited to any prime traceability matrix changes or subcontractor matrix changes (e.g. each subcontractor award or scope change or QMS change) for approval.	
Preparation Information: The MAIP shall cover all MAR requirements and be applicable to: - 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 - 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 an up-to-date traceability matrix to planned processes for all mission assurance requirements for the prime and suppliers. Specifically, the prime shall document supplier compliance by showing which MAR requirements were allocated to each supplier and how the allocated requirements will be met by each supplier and include these plans in their overall MAIP. Note: supplier documentation may take the form of individual supplier MAIPs, with compliance matrices, referred to in the overall MAIP compliance matrix or individual compliance matrices for each supplier attached to the overall MAIP depending on supplier criticality.	

DID 1-1B Product Assurance Implementation Plan (Instrument subsystem Only)

Title: Product Assurance Implementation Plan (Instrument subsystem Only)	DID1-1b
Reference: ICESat-2 MAR Paragraph 1.1	
Use: Documents the developer's plan for implementing a system safety and mission assurance program	
Related Documents:	
Place/Time/Purpose of Delivery: - Delivered to the Project Office sixty (60) days after contract delegation of responsibility/requirements. - Updates shall be delivered to the Project Office within thirty (30) days of plan changes including but not limited to any traceability matrix for approval.	

Preparation Information:

Each developer shall submit for review and approval a Product Assurance Implementation Plan (PAIP), section 1.1, in accordance with the requirements of the ICESAT-2 MAR (Mission Assurance Requirements). The PAIP shall include:

1. An overview of the developer's plan for accomplishing the assurance activities required by this MAR.
2. A specific and detailed description of how the performance assurance requirements are to be accomplished. Reference documents that provide the required details shall be submitted with the PAIP.
3. A list of any unmet requirements to the MAR including supporting rationale and details of the developer's alternate approach, if any, to meet the specific MAR requirement shall be provided.
4. 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
5. The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items

The PAIP shall include an up-to date traceability matrix traceability matrix for the mission assurance requirements, referring to the developer's Quality Manual and supporting documentation.

DID 1-2 PREVIOUSLY DEVELOPED PRODUCT – COMPLIANCE WITH REQUIREMENTS

Title: Previously Developed Product – Compliance with Requirements	DID 1-2
Reference: ICESat-2 MAR Paragraph 1.2	
Use: Documents the compliance of previously developed product with the requirements of the SOW and the MAIP	
Related Documents: Mission Assurance Implementation Plan	
Place/Time/Purpose of Delivery: - Delivered to the Project Office thirty 30 days after identification of the previously developed product for approval	
Preparation Information: The document shall identify the 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 a waiver or deviation.	

DID 2-1 QUALITY MANUAL

Title: Quality Manual	DID 2-1
Reference: MAR Paragraph 2.0	
Use: Documents the developer's quality management system.	
Related Documents: - SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing - ISO 10013 Quality Manual Development Guide	
Place/Time/Purpose of Delivery: - Provide with proposal for GSFC review - Provide updates to the project office 30 days after contract award for review	
Preparation Information: Prepare a Quality Manual addressing applicable requirements of AS9100; refer to ISO 10013 Quality Manual Development Guide for guidelines on preparation of a quality manual.	

DID 2-2 REPORTING OF MRB ACTIONS

Title: Reporting of MRB Actions	DID 2.2
Reference: ICESat-2 MAR Paragraph 2.4	
Use: Report MRB actions to the project office.	
Related Documents: - SAE AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing	
Place/Time/Purpose of Delivery: This DID is for documentation only. Notification is within 24 hours. - 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 relevant information on a developer MRB form that includes at least the following: - Identification of project, system, or sub-system - Identification of item (e.g., assembly, sub-assembly, or part, to include serial number or part number as applicable) - Description of affected item - Definition of major and minor nonconformances - Identification of next higher assembly - Description of anomaly, including activities leading up to the anomaly - Names and contact information of involved individuals - Status of item - Contact information for personnel who originated the report - Date of original submission to the MRB - Actions taken after approval	

DID 2-3 REQUEST FOR A DEVIATION OR WAIVER

Title: Request for a deviation or waiver	DID 2-3
Reference: ICESat-2 MAR Paragraph 2.3	
Use: Request government approval of a deviation or waiver.	
Related 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 deviation or 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 2-4 Anomaly Report

Title: Anomaly Report	DID 2-4
Reference: ICESat-2 MAR Paragraph 2.1	
Use: Document anomalies, investigative activities, rationale for closure, and corrective and preventive actions	
Related 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 - Deliver all record in the electronic format specified below as part End item data packages (EIDP) as specified in DID16-1.	
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—mission impact and certainty in corrective actions	

DID 3-1 SYSTEM SAFETY PROGRAM PLAN

Title: System Safety Program Plan	DID No.: 3-1
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
- AFSPCMAN 91-710, Range Safety User Requirements, Volume 1, Attachment 2, Para. A2.2.2

Place/Time/Purpose of Delivery:

- Deliver Preliminary to the Project Office at SRR for approval.
- Deliver Final to the Project Office forty-five (45) days prior to PDR for approval.

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. This includes hazards associated with safety critical software as described in Section 5.2.1 of this MAR.
- 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 3-2 SAFETY REQUIREMENTS COMPLIANCE CHECKLIST

Title: Safety Requirements Compliance Checklist	DID No.: 3-2
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 3-10.	
Reference Documents: - AFSPCMAN 91-710, Range Safety User Requirements - Reference MAR Section 3.1.1, Mission Related Safety Requirements Documentation	
Place/Time/Purpose of Delivery: - Deliver to the Project Office forty-five (45) days prior to PDR for approval. - Deliver Final 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 - Resolution - Reference - Copies of all Range Safety and NASA approved non-compliances including waivers and equivalent levels of safety certifications	

DID 3-3 PRELIMINARY HAZARD ANALYSIS

Title: Preliminary Hazard Analysis	DID No.: 3-3
MAR Paragraph: 3.3.4	
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, probability, 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: - AFSPCMAN 91-710, Range Safety User Requirements, Volume 1, Attachment 2, Para. A2.2.3 - NPR 8715.7, ELV Payload Safety Program - MIL-STD-882E, Standard Practice for System Safety, Appendix B - NASA-STD-8719.13, NASA Software Safety Standard	
Place/Time/Purpose of Delivery: ***Tailoring note: delete the non-applicable requirement*** - Submit the PHA with the Preliminary ISAR (DID 3-7) to the Project Office for approval. - Submit the PHA with the SDP I (DID 3-7) 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. 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; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage). 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 3-4 OPERATIONS HAZARD ANALYSIS

Title: Operations Hazard Analysis	DID No.: 3-4
MAR Paragraph: 3.3.5	

Use:

The Operations Hazard Analysis (OHA) 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 Verification Tracking Log to the Project Office forty-five (45) days prior to Systems Integration Review or Pre-Environmental Review for approval.

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 3-5 SAFETY HAZARD ANALYSIS ON CRITICAL LIFT EQUIPMENT

Title: Safety Hazard Analysis on Critical Lift Equipment	DID No.: 3-5
MAR Paragraph: 3.4	
Use: A recognized safety hazard analysis, such as fault tree analysis, FMEA, Operating and Support Hazard Analysis (O&SHA), shall be performed on all lifting devices used for critical lifts. The analysis shall, as a minimum, 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.	
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: • The analysis shall be performed as part of the initial evaluation process for critical lift compliance and prior to use in a critical lift, included in the crane documentation, and updated as required to reflect any changes in operation and/or configuration. • It shall be submitted to the Project Office for approval	
Preparation Information:	

DID 3-6 OPERATING AND SUPPORT HAZARD ANALYSIS

Title: Operating and Support Hazard Analysis (O&SHA)	DID No.: 3-6
MAR Paragraph: 3.4.1	
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: - AFSPCMAN 91-710, Range Safety User Requirements, Volume 1, Attachment 2, Para A2.2.4.3 - 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 Intermediate & Final ISARs (DID 3-7). - Deliver the results of the O&SHA to the Project Office as a part of the SDP II & SDP III (DID 3-7).	

DID 3-7 INSTRUMENT SAFETY ASSESSMENT REPORT

Title: Instrument Safety Assessment Report (ISAR)	DID No.: 3-7
MAR Paragraph: 3.4.2	

Use:

The Instrument Safety Assessment Report (ISAR) documents the comprehensive evaluation of the risk being assumed prior to the testing or operation of an instrument. The spacecraft developer will use the ISAR as an input to the Safety Data Package (SDP).

Reference Documents:

- AFSPCMAN 91-710, Range Safety User Requirements, Volume 1, Attachment 2, Para. A2.2.5
- JSC 26943 Guidelines for the Preparation of Payload Flight Safety Data Packages and Hazard Reports
- NASA-STD-8719.13, NASA Software Safety Standard

Place/Time/Purpose of Delivery:

- Deliver the Preliminary ISAR to the Project Office thirty (30) days prior to instrument PDR for approval.
- Deliver the Intermediate ISAR to the Project Office thirty (30) days prior to instrument CDR for approval.
- Deliver a draft of the Final ISAR to the Project Office thirty (30) days prior to instrument PER for review and the Final ISAR thirty (30) days prior to instrument PSR for approval

Preparation Information:

The ISAR will identify safety features of the hardware, software, and system design as well as procedural, hardware, and software related hazards that may be present in the instrument. This includes specific procedural controls and precautions that should be followed. The ISAR will include the following information:

- The safety criteria and methodology used to classify and rank hazards, including assumptions upon which the criteria or methodologies were based or derived
- The results of hazard analyses and tests used to identify hazards in the system including:
- Those hazards that still have a residual risk and the actions that have been taken to reduce the associated risk to a level contractually specified as acceptable
- Results of tests conducted to validate safety criteria, requirements, and analyses
- Hazard reports documenting the results of the hazard analyses to include a list of all significant hazards along with specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment. NOTE: Identify whether or not the risks may be expected under normal or abnormal operating conditions.
- Any hazardous materials generated by or used in the system
- The conclusion, including a signed statement, that all identified hazards have been eliminated or their associated risks controlled to levels contractually specified as acceptable and that the instrument is ready to test, operate, or proceed to the next phase
- In order to aid the spacecraft developer in completing an orbital debris assessment of the instrument it is necessary to identify any stored energy sources in instruments (pressure vessel, Dewar, etc.) as well as any energy sources that can be passivated at end of life.

DID 3-7 SAFETY DATA PACKAGE

Title: Safety Data Package (SDP)	DID No.: 3-8

MAR Paragraph: 3.4.3

Use:

The SDP provides a description of the payload 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 or instrument Project Manager shall demonstrate compliance with these requirements and shall certify to GSFC and the launch range, through the SDP, that all safety requirements have been met.

Reference Documents:

- AFSPCMAN 91-710, Range Safety User 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 3-2).

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 on the probability of occurrence and severity level of potential mishaps.
      iii. A discussion of the residual risks that remain after the controls are applied or for which no controls could be applied.
      iv. 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. An assessment of the results of the safety program efforts; a list of significant hazards and specific safety recommendations to ensure the safety of personnel and property.
   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 3-8 VERIFICATION TRACKING LOG

Title: Verification Tracking Log	DID No.: 3-9
MAR Paragraph: 3.4.4	

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.

Reference Documents:

- AFSPCMAN 91-710, Range Safety User Requirements
- KHB 1700.7, Space Shuttle Payload Ground Safety Handbook
- RSM-93, WFF Range Safety Manual for Goddard Space Flight Center (GSFC)

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 final ISAR (DID 3-7) for review.
- 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 (3-7) 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 operational use or restraint.

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 launch site range safety requirements.

The VTL shall contain the following information in tabular format:

- Hazard Report #
- Safety Verification #
- 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 3-9 HAZARDOUS PROCEDURES FOR PAYLOAD I&T AND PRE-LAUNCH PROCESSING

Title: Hazardous Procedures for Payload I&T and Pre-launch Processing	DID No.: 3-10
MAR Paragraph: 3.4.5	
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) - AFSPCMAN 91-710, Range Safety User Requirements, Volume 6, Attachment 2 - 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 3-10 SAFETY WAIVER

Title: Safety Waiver	DID No.: 3-11
MAR Paragraph: 3.4.6	

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 Range Safety 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/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 3-11 ORBITAL DEBRIS ASSESSMENT REPORT (ODAR) AND END OF MISSION PLAN (EOMP) INPUTS

Title: Orbital Debris Assessment Report (ODAR) and End Of Mission Plan (EOMP) Inputs	DID No.: 3-12
MAR Paragraph: 3.4.7	
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 inputs to the Project Office fifteen (15) days prior to mission PDR. - Deliver interim inputs to the Project Office sixty (60) days prior to mission CDR. - Deliver the final/updated inputs to the Project Office 90 days prior to PSR..	
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 3-12 PRE-MISHAP PLAN

Title: Pre-Mishap Plan	DID No.: 3-13
MAR Paragraph: 3.4.8	
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 t.	
Reference Documents: - NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping	
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 and control a mishap or a close call, as well as identify the chain of individuals (including Project Office personnel) to be contacted in the event a mishap or close call occurs.	

DID 3-13 MATERIAL SELECTION LIST FOR PLASTIC FILMS, FOAMS, AND ADHESIVE TAPES

Title: Material Selection List for Plastic Films, Foams, and Adhesive Tapes	DID No.: 3-14
MAR Paragraph: 3.4.9	
Use: Submitted to Launch Range Safety for assessment of flammability.	
Reference Documents: - KTI-5212 Material Selection List for Plastic Films, Foams, and Adhesive Tapes	
Place/Time/Purpose of Delivery: - Deliver to the Project Office with the Final ISAR (DID 3-7) for review. - Deliver to the Project Office with the SDP III (DID 3-7) for review	
Preparation Information: The developer shall complete form KTI-5212 Material Selection List for Plastic Films, Foams, and Adhesive Tapes. NOTE: Material Selection Forms are available for download from ELV Payload Safety Program website at URL: http://ksc-sma.ksc.nasa.gov/ELVPayloadSafety/Requirements.html	

DID 3-14 RADIATION FORMS AND ANALYSES

Title: Radiation Forms and Analyses	DID No.: 3-15
MAR Paragraph: 3.4.9	

Use:

The forms and analyses support the NASA launch safety approval process.

Reference Documents:

- KNPR 1860.1 KSC Ionizing Radiation Protection Program
- KNPR 1860.2 KSC Non-Ionizing Radiation Protection Program

Place/Time/Purpose of Delivery:

Tailoring note: delete the non-applicable requirement:

- Deliver to the Project Office with the Final ISAR (DID 3-7) for review.
- Deliver to the Project Office with the SDP III (DID 3-7) for review.

Preparation Information:

The developer shall prepare the following forms per the requirements of NPR 8715.3:

- 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

NOTE: Radiation Forms are available for download from ELV Payload Safety Program website at URL:

http://kscsma.ksc.nasa.gov/ELVPayloadSafety/Forms.html

DID 3-15 PROCESS WASTE QUESTIONNAIRE

Title: Process Waste Questionnaire	DID No.: 3-16
MAR Paragraph: 3.4.9	
Use: The forms and analyses support the NASA launch safety approval process.	
Reference Documents:	
Place/Time/Purpose of Delivery: - Deliver to the Project Office with the Final ISAR (DID 3-7) for review. - Deliver to the Project Office with the SDP III (DID 3-7) for review.	
Preparation Information The developer shall complete KSC Form 26-551V2 Process Waste Questionnaire.	

DID 3-16 ENVIRONMENTAL IMPACT STATEMENT

Title: Environmental Impact Statement	DID No.: 3-17
MAR Paragraph: 3.4.9	
Use: The forms and analyses support the NASA launch safety approval process.	
Reference Documents:	
Place/Time/Purpose of Delivery: - Deliver to the Project Office with the Final ISAR (DID 3-7) for review. - Deliver to the Project Office with the SDP III (DID 3-7) for review.	
Preparation Information The developer shall complete AF Form 813 Request for Environmental Impact Analysis.	

DID 4-1 PROBABILISTIC RISK ASSESSMENT (PRA) AND RELIABILITY PROGRAM PLAN

Title: PRA and Reliability Program Plan	DID 4-1
Reference: ICESat-2 MAR Paragraph 4.0	
Use: Planning and implementation of Probabilistic Risk Assessment (PRA) and reliability activities.	
Related Documents: - NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy - NASA-STD-8729.1, Planning, Developing and Managing an Effective Reliability and Maintainability (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 plans to the Project Office sixty (60) days after contract award for review - Deliver final plans to the Project Office thirty (30) days prior to the Systems Requirements Review for approval - Deliver activity reports related to implementation of the plans at milestone reviews beginning with the Systems Requirements Review for review	
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 4-2: PROBABILISTIC RISK ASSESSMENT

Title: Simplified Probabilistic Risk Assessment	DID 4-2
Reference: ICESat-2 MAR Paragraph 4.1.1	
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.	
Related Documents - NPR 8705.4 Risk Classification for NASA Payloads - NPR 8705.5 Probabilistic Risk Assessment (PRA) Procedures 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 interim report to the Project Office thirty (30) days prior to Observatory PDR for review. - Deliver PRA support data thirty (90) days prior to Elemental (i.e., Bus, ATLAS) PDR for review and incorporation in system-level analyses. - Deliver updated interim report to the Project Office thirty (30) days prior to CDR for review. - Deliver PRA support data thirty (90) days prior to Elemental (i.e., Bus, ATLAS) CDR for review and incorporation in system-level analyses. - Deliver updated interim report to the Project Office thirty (30) days prior to MOR for review. - Deliver final report to the Project Office thirty (30) days prior to FOR for approval.	
Preparation Information: The PRA shall be performed at the system/observatory level 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. Supporting PRA supporting data (i.e., event state definitions, fault trees, FMEAs, etc.) shall be supplied by system element teams (i.e., Spacecraft Bus, Each Payload, Etc.)	

DID 4-3: FAILURE MODE AND EFFECTS ANALYSIS AND CRITICAL ITEMS LIST

Title: Failure Mode and Effects Analysis (FMEA) and Critical Items List (CIL)	DID 4-3
Reference: ICESat-2 MAR Paragraph 4.1.2	
Use: Used to evaluate design against requirements, to identify single point failures and hazards, and to identify modes of failure within a system design including hardware and software, for the early mitigation of potential catastrophic and critical failures.	
Related Documents - GSFC Flight Assurance Procedure, FAP P-322-208, Performing a Failure Mode and Effects Analysis - NPR 8705.4 Risk Classification for NASA Payloads	
Place/Time/Purpose of Delivery: - Deliver preliminary FMEA to the Project Office thirty (90) days before PDR for review - Deliver final FMEA to the Project Office thirty (90) days prior to CDR for approval - Deliver updated FMEA and CIL to the Project Office thirty (days) prior to each subsequent milestone review leading up to Launch for approval	
Preparation Information: The FMEA 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 - Single-point failure analysis, to include the root cause, mitigation, and retention rationale for those with severity categories 1, 1R, 1S, 2, 2S or 2R. - 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, 2, and 2R, including item identification, cross-reference to FMEA line items, and retention rationale. Appropriate retention rationale may include design features, historical performance, acceptance testing, manufacturing product assurance, elimination of undesirable failure modes, and failure detection methods.	

DID 4-4: FAULT TREE ANALYSIS

Title: Fault Tree Analysis (FTA)	DID 4-4

Reference:

ICESat-2 MAR Paragraphs 4.2

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.

Related 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 (90) days prior to PDR for review.
- Deliver final qualitative mission FTA report to Project Office thirty (90) 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 including hardware and software,
- Results and conclusions

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

DID 4-5: PARTS STRESS ANALYSIS

Title: Parts Stress Analysis	DID 4-5

Reference:

ICESat-2 MAR Paragraph 4.3

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.

Related 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 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 4-6: WORST CASE ANALYSIS

Title: Worst Case Analysis	DID 4-6
Reference: ICESat-2 MAR Paragraph 4.4	
Use: Demonstrate design margins in electronic and electrical circuits, optics, and electromechanical and mechanical items.	
Related Documents - NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy - NASA-STD-8729.1, Planning, Developing and Managing an Effective R&M Program. - 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 4-7: RELIABILITY ASSESSMENTS AND PREDICTIONS

Title: Reliability Assessments and Predictions	DID 4-7
Reference: ICESat-2 MAR Paragraph 4.5	
Use: Used to assist in evaluating alternative designs and to identify potential mission limiting elements that may require special attention.	
Related Documents: - IEEE Standard Methodology for Reliability Prediction and Assessment for Electronic Systems and Equipment – Std 1413 - RADC-TR-85-229, Reliability Prediction for Spacecraft	
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 to Project Office thirty (30) days prior to PDR for review - Deliver final report to Project Office thirty (30) days prior to CDR for review	
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 4-8 LIMITED-LIFE ITEMS LIST

Title: Limited-Life Items List	DID 4-8
Reference: ICESat-2 MAR Paragraph 4.8	
Use: Tracks the selection and application of limited-life items and the predicted impact on mission operations	
Related 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 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 5-1: SOFTWARE ASSURANCE PLAN

Title: Software Assurance Plan	DID 5-1

Reference:

ICESat-2 MAR Paragraph 5.1

Use:

Documents the developers Software Quality Assurance roles and responsibilities, and surveillance activities to be performed as outlined in the NASA Software Assurance Standard.

Related Documents:

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

Place/Time/Purpose of Delivery:

- Deliver preliminary plan to the Project Office thirty (30) days after the beginning of Phase B for review
- Deliver baseline plan to the Project Office fifteen (15) days prior to PDR for approval
- Deliver updates to the Project Office fifteen (15) days prior to implementation for approval

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
    - Software Inventory Worksheet
    - Independent Verification and Validation (if applicable)
- Assurance tools, techniques, and methodologies
- Software Assurance Program Metrics
- Problem Reporting and Corrective Action
- Assurance records, collection, maintenance, and retention
- Training
- Risk Management
- SQAP Change procedure and history

DID 5-2: SOFTWARE ASSURANCE STATUS REPORT

Title: Software Assurance Status Report	DID 5-2
Reference: ICESat-2 MAR Paragraph 5.5	
Use: Software Assurance Status Report provides information regarding the developer's assurance activities, accomplishments, significant problems, and future plans.	
Related Documents: - NASA-STD-8739.8, NASA Standard for Software Assurance - 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 include 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 - Lessons Learned	

DID 6-1 GROUND SYSTEMS MISSION ASSURANCE IMPLEMENTATION PLAN

Title: Ground Systems Mission Assurance Implementation Plan	DID 6-1
Reference: ICESat-2 MAR PARAGRAPH 6.1	
Use: Documents the developer's mission assurance implementation plan for ground systems.	
Related Documents: - NASA-STD-8719.9 Standard for Lifting Devices and Equipment - GSFC-STD-1000 Rules for the Design, Development, Verification, and Operation of Flight Systems	
Place/Time/Purpose of Delivery: - Deliver to Project Office thirty (30) days after contract award for approval	
Preparation Information: The developer's plan shall address the ground systems and equipment requirements with respect to procurement, development, test, operation, and maintenance for both ground systems and flight systems. The plan shall address support to flight items to the extent necessary to assure functional integrity of flight items, including health and safety.	

DID 6-2 MISSION OPERATIONS EQUIPMENT PLAN

Title: Mission Operations Center Equipment Plan	DID 6-2
Reference: ICESat-2 MAR Paragraph 6.1	
Use: Documents the developer's plans for developing, building, and maintaining ground operations equipment to support launch and flight operations.	
Related Documents: - NASA-STD-8719.13 NASA Software Safety Standard - NASA-STD-8739.8 NASA Standard for Software Assurance - NPR 8705.4 Risk Classification for NASA Payloads - NPR 8705.5 PRA Procedures for NASA Programs and Projects	
Place/Time/Purpose of Delivery: - Deliver to the GSFC Project Office fifteen (15) days prior to mission MOCC PDR for review - Deliver to the GSFC Project Office fifteen (15) days prior to mission MOCC CDR for approval	
Preparation Information: The developer shall address the following: - Functions necessary to support launch and flight operations - Requirements definition, management, traceability, and verification - Verification and validation - Acceptance criteria - Configuration control (functional and physical) - Interface control drawings - Critical Interfaces - Testing—unit testing, integration and test, system level, acceptance test, interface, end-to-end testing, compatibility testing, data flow testing, mission simulations, regression testing and operational readiness testing - User/operational manuals - Control center and flight operations Failure Modes and Effects Analysis Support - Software Code walkthroughs and reviews - Trend data - Controls to prevent actions or events that threaten mission success - Equipment Failures - Control center availability (redundancy, repair, spares, sparing) - Contingency plans and procedures - Acceptance testing, end-to-end, compatibility testing, data flow and operational readiness testing, including appropriate support from ground data system elements to demonstrate operational compatibility of system to perform as required	

DID 7-1 RISK MANAGEMENT PLAN

Title: Risk Management Plan	DID 7-1
Reference: ICESat-2 MAR Paragraph 7.0	
Use: Defines the process by which the developer identifies, evaluates, and mitigates the risks associated with program, project, and/or mission goals	
Related Documents: - NPR 8000.4, Risk Management Procedures and Guidelines	
Place/Time/Purpose of Delivery: - Deliver to the Project Office sixty (60) after contract award for approval	

Preparation Information:

The Risk Management Plan shall include:

- Description of contract requirements
- Purpose and Scope
- Assumptions, Constraints, and Policies
- Related 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 shall 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 and Reporting

DID 7-2 RISK LIST

Title: Risk List	DID 7-2
Reference: ICESat-2 MAR Paragraph 7.3	
Use: Defines the documentation and reporting of risk items.	
Related Documents: - GID 7120.2 GSFC 5x5 Risk Matrix - NPR 8000.4, Agency Risk Management Procedural Requirements	
Place/Time/Purpose of Delivery: - Deliver Monthly Status Reports/List Updates - Deliver to the Project Office fifteen (15) days prior to each milestone reviews beginning with PDR for review	

Preparation Information:
Prepare a prioritized list of risks that includes
- Identification number
- Title
- Current approach (mitigate, watch, accept, research)
- Rank
- Trend
 	
Prepare a chart for each risk that includes:
- Identification number
- Title
- Rank
- Risk statement (condition-consequence form)
- Brief discussion of:
  - Current approach
  - Actions causing change
  - Current status	

DID 8-1 SYSTEMS REVIEW MATERIALS

Title: Systems Review Materials	DID 8-1
Reference: ICESat-2 MAR Paragraph 8.0	
Use: To provide the systems review team with the materials used to conduct the review.	
Related Documents - Project Systems Review Plan (ICESat2-0051) GSFC-STD-1001 Criteria for Flight and Flight Support Systems Lifecycle Reviews	
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 related documents.	

DID 8-2 ACTION ITEM RESPONSES

Title: Action Item Responses	DID 8-2
Reference: ICESat-2 MAR Paragraph 8.0	
Use: To respond to action items resulting from the review.	
Related Documents - Project Systems Review Plan (provided by Project Office) - GSFC-STD-1001 Criteria for Flight Project Critical Milestone ReviewsCriteria for Flight and Flight Support Systems Lifecycle Reviews	
Place/Time/Purpose of Delivery: - Provide response to action items to the Project Office thirty (30) days after end of review for approval	
Preparation Information: See the guidelines presented in the related documents.	

DID 8-3 PEER REVIEW PROGRAM

Title: Engineering Peer Review Program	DID 8-3
Reference: ICESat-2 MAR Paragraph 8.1	
Use: The ERP Plan shall provide a detailed plan defining how the contractor will establish, conduct, and document component/subsystem level EPRs. EPRs are focused, in-depth technical reviews used to provide confirmation and offer options by bringing in experts early and at appropriate points throughout the life cycle. The reviews provide a table-top examination of requirements, interfaces, design, analysis, manufacturing, integration, test and operational details, drawings, processes, and data.	
Related Documents: NPR7120.5D Spaceflight Program and Project Management Requirements , GPR 8700.6B Engineering Peer Reviews	
Place/Time/Purpose of Delivery: - Provide to the Project Office sixty (60) days after contract award for approval	
Preparation Information: The EPR Plan document, at a minimum, shall consist of: 1. Review content and requirements. 2. Definition of the members. 3. Definition of the Peer Review process 4. How action items and responses will be documented, tracked, and closed in compliance with the SOW. The Engineering Peer Review Plan shall be consistent with the ICESat-2 Engineering Peer Review Plan.	

DID 9-1 SYSTEM PERFORMANCE VERIFICATION PROGRAM PLAN

Title: System Performance Verification Program Plan	DID 9-1

Reference:

ICESat-2 MAR Paragraph 9.0

Purpose:

Provides the overall approach for accomplishing the verification program. Defines the specific tests, analyses, calibrations, alignments, hardware models, etc. that will demonstrate that the flight hardware complies with the mission requirements.

Related Documents:

- GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects
- ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document

Place/Time/Purpose of Delivery:

- Provide preliminary plan to Project Office ninety (90) days after contract award for review
- Provide final plan to Project Office thirty (30) days prior to CDR for approval

Preparation Information:

The System Performance Verification Program Plan shall be prepared to comply with the requirements of paragraph 2.1.1.1 of GSFC-STD-7000. The Observatory Performance Verification Plan (OPVP) shall be provided in accordance with ICESat-2 MAR DID 9-1 and include the following:

A. Be separated into sections such that it is clear which spacecraft requirements are verified at the spacecraft and Observatory levels.

B. Flow performance requirements to all levels of assembly and describe the verification method for these tests.

The OPVP describes the approach (test, analysis, etc.) that will be utilized to verify performance against the requirements documents (SRD, ATLAS-SC IRD, LSIRD, MAR, EVR). The plan shall detail the series of functional demonstrations, analytical investigations, physical property measurements, and tests that simulate the environments encountered during handling, transportation, pre-launch, and on-orbit operations. The plan also covers the engineering design and performance analyses and tests of the spacecraft and its components and sub-systems. The plan shall clearly define the specific tests and analyses that will collectively demonstrate that the hardware and software complies with the functional, performance, and operational requirements of the ICESat-2 Program specifications. If verification relies on measurements, tests, or analyses at lower (or other) levels of assembly, this dependence shall be described.

The plan shall include:

1. System Engineering design analysis, simulations and analysis of test data
2. Component design verification, including environmental tests planned, workmanship verification and any unique requirements for each component.
3. Subsystem design verification, including developmental tests, engineering tests, mathematical models, computer simulations and hardware models that will be used to demonstrate the acceptability of the spacecraft or ground unit design.
4. Mechanical function verification, with emphasis on appendage deployment and articulation systems, including analyses, computer simulations, development tests, engineering tests, engineering hardware, design qualification tests, life tests, and acceptance tests. Tests to be performed during spacecraft assembly shall be included in the I&T Plan.
5. Performance verification tests and test matrices for all levels of assembly.
6. Design and functional verification under the specified environmental requirements.
7. Verification specifications that stipulate the specific environmental tests and monitoring parameters associated with each test and analysis in the plan.
8. Specific test and analytical parameters associated with each test shall be defined in the plan.

DID 9-2 ENVIRONMENTAL VERIFICATION PLAN

Title: Environmental Verification Plan	DID 9-2
Reference: ICESat-2 MAR Paragraph 9.1	
Purpose: The Environmental Verification Plan documents the contractor's approach for environmental qualification and acceptance tests. The Environmental Test Matrix summarize the tests performed. This DRD also satisfies the environmental verification requirements of the launch services provider.	
Related Documents: - GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects - ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document	
Place/Time/Purpose of Delivery: - Provide preliminary plan to Project Office ninety (90) days after contract award for review - Provide final plan to Project Office thirty (30) days prior to CDR for approval	
Preparation Information: The Environmental Verification Plan shall be provided in accordance with ICESat-2 MAR DID 9-2. It shall provide the general test philosophy and an overview of the systems-level environmental testing to be performed to demonstrate that the hardware and software comply with the environmental verification requirements. The verification plan shall include test objectives, test specimen configuration, general test methods, and a schedule. It should not include detailed test procedures. The environmental verification plan shall provide the overall approach to accomplishing the environmental verification program. For each test, it shall include the level of assembly, the configuration of the item, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, necessary functional operations, personnel responsibilities, and requirement for procedures and reports. It shall also define a rationale for retest determination that does not invalidate previous verification activities. When appropriate, the interaction of the test and analysis activity shall be described. Limitations in the environmental verification program 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.

The Environmental Verification Plan shall have separate sections for the instrument and the spacecraft.

As an adjunct to the environmental verification plan, an environmental test matrix shall be prepared provided in accordance with ICESat-2 MAR DID 9-4 and shall summarize all tests that will be performed on each component, each subsystem, and the payload. The purpose is to provide a ready reference to the contents of the test program in order to prevent the deletion of a portion thereof without an alternative means of accomplishing the objectives; it has the additional purpose of ensuring that all flight hardware has been subjected to environmental exposures that are sufficient to demonstrate acceptable workmanship. 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.

The Environmental Verification Plan shall be provided in accordance with ICESat-2 MAR DID 9-2. It shall provide the general test philosophy and an overview of the systems-level environmental testing to be performed to demonstrate that the hardware and software comply with the environmental verification requirements.

The verification plan shall include test objectives, test specimen configuration, general test methods, and a schedule. It should not include detailed test procedures.

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

Limitations in the environmental verification program 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.

The Environmental Verification Plan shall have separate sections for the instrument and the spacecraft.

DID 9-3 SYSTEM PERFORMANCE VERIFICATION MATRIX

Title: System Performance Verification Matrix	DID 9-3
Reference: ICESat-2 MAR Paragraph 9.2	
Use: Establishes the System Performance Verification Matrix.	
Related Documents: - GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects - ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document	
Place/Time/Purpose of Delivery: - The updated System Performance Verification Matrix shall be included in the data packages for the Integrated Independent Reviews, beginning with PDR, for review	
Preparation Information: The System Performance Verification Matrix (SPVM) shall be provided in accordance with ICESat-2 MAR DID 9-3 and shall summarize the flow-down of system specification, Mission Assurance, and calibration/validation requirements verification. The SPVM shall stipulate how each requirement will be verified, and summarizes current status of compliance/non-compliance with requirements. The SPVM shall list a summary description of each requirement, and a summary of the measured/analyzed/demonstrated performance of the system against each requirement. It shall show each Requirements Document, requirement reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, report reference numbers, etc. for each requirement set from the Requirements Document. It shall show the flow-down of requirements verification through the sub-system (box/board) level. The SPVM shall trace requirements backwards to the next level above, i.e., a level 4 requirement shall be traced back to its level 3 parent, etc	

DID 9-4 ENVIRONMENTAL TEST MATRIX

Title: Environmental Test Matrix	DID 9-4
Reference: ICESat-2 MAR Paragraph 9.3	
Use: Establishes a matrix that summarizes the environmental tests and test status for flight hardware and other equipment.	
Related Documents: - GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects - ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document	
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: As an adjunct to the environmental verification plan, an environmental test matrix shall be prepared provided in accordance with ICESat-2 MAR DID 9-4 and shall summarize all tests that will be performed on each component, each subsystem, and the payload. The purpose is to provide a ready reference to the contents of the test program in order to prevent the deletion of a portion thereof without an alternative means of accomplishing the objectives; it has the additional purpose of ensuring that all flight hardware has been subjected to environmental exposures that are sufficient to demonstrate acceptable workmanship. 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, subsystem, or payload (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 9-5 VERIFICATION REPORTS

Title:	CDRL No.:
Verification Reports	9-5

Reference:

ICESat-2 MAR Paragraph 9.4

Use:

Report the results of all tests identified in the Test Plans, including test procedures used, test results, and configuration status of all items under test.

Related Documents:

- GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects
- ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document

Place/Time/Purpose of Delivery:

- Preliminary verification report shall be provided to Project Office within 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

Preparation Information:

The Contractor shall provide formal written test reports that summarize the results of verification tests on the observatory for the following testing: EMI/EMC, Vibe, Acoustic, Thermal Vacuum, Alignment.

The Contractor shall provide post-test reviews with the Government to analyze the expected results.

The following shall be included in test reports:

a. Test identification and hardware configuration for specific tests
b. Facility description
c. Reference applicable test plan, test procedures, and test requirements, test log including the dates of the testing, photographs of test setup, any malfunction reports written during the test
d. Test results, to include:

    1. Identification of test results which confirmed the expected results as specified in the test plan / procedures or for which variations between actual and expected results were within specified tolerance. For the latter case, actual test results shall be shown.

    2. Identification of test results which differ from expected results beyond expected or acceptable limits

    3. Identification of any planned test objective or requirement for which actual results were not obtained. Reasons for not meeting the objective/requirement shall be stated.

4. Identification of any false or aberrant results noted during the test or subsequent analyses. Note that any such behavior that can prevent the spacecraft from accomplishing its mission objectives can be a basis for rejection.

5. A copy of the as-run test procedure(s)

6. Test data for analysis as requested

e. Recommendations for subsequent actions shall be stated, based on the test results, to include:

1. Redesign of a particular component to enable the spacecraft to meet a specific requirement which was not fulfilled

DID 9-6 SYSTEM PERFORMANCE VERIFICATION REPORT

Title: System Performance Verification Report	CDRL No.: 9-6
Reference: ICESat-2 MAR Paragraph 9.5	
Use: Establishes a Performance Verification Report that compares hardware/software specifications with the final verified values.	
Related Documents: - GSFC-STD-7000 General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects - ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document	
Place/Time/Purpose of Delivery: - Updated reports shall be provided with the review data package at milestone reviews, beginning with PDR, for information - The final report shall be submitted within thirty (30) days after completion of on-orbit checkout for information	
Preparation Information: The System Performance Verification Report shall be prepared and maintained per paragraph 2.1.1.6 of GSFC-STD-7000.	

DID 10-1 ESD CONTROL PLAN

Title: ESD Control Plan	CDRL No.: 10-1
Reference: ICESat-2 MAR Paragraph 10.2	
Use: Implementation of an ESD control program at the developer's facility	
Related 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 review	

DID 10-2 CONTAMINATION CONTROL PLAN AND DATA

Title: Contamination Control Plan and Data	DID 10-2

Reference:

ICESat-2 MAR Paragraph

10.3.1

Use:

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

Related Documents:

- GSFC-STD-7000 General Environmental Verification Standard (GEVS)
- ICESat-2-SYS-REQ-0011, ICESat-2 Environmental Description Document
- 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 16-1)

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 contamination 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 11-1: PARTS CONTROL PROGRAM

Title:	DID No.:
Parts Control Program	11-1

Reference:

ICESat-2 MAR Paragraph 11.0

Use:

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

Related Documents

- GSFC EEE-INST-002 Instructions for EEE Parts Selection, Screening, Qualification, and Derating
- S-311-M-70 Specification for Destructive Physical Analysis

Place/Time/Purpose of Delivery:

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

Preparation Information:

The PCP shall address the following:

- Shelf life control plan
- Parts application derating
- Supplier and manufacturer surveillance
- Qualification
- ASICs, Gate Arrays, System-on-chip, Custom ICs
- Incoming inspection and test
- Destructive Physical Analysis
- Defective parts controls program.
- Radiation hardness assurance
- Handling, preservation, and packing
- Contamination control
- Alternate quality conformance inspection and small lot sampling
- Traceability and lot control
- Failure analysis

DID 11-2: PARTS CONTROL BOARD

Title:	DID No.:
Parts Control Board	11-2
Reference:	
ICESat-2 MAR Paragraph 11.1	
Use:	
Organization and operation of the Parts Control Board regarding the implementation of the Parts Control Program.	
Related 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 approval.	
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 11-3: Parts Identification List

Title: Parts Identification List (PIL)	DID 11-3
Reference: ICESat-2 MAR Paragraph 11.3	
Use: A list of EEE parts that may be selected for use in flight hardware.	
Related 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: - Flight component identity to the circuit board level - Complete part number (i.e. DSCC part number, SCD part number, with all suffixes) - Manufacturer's Generic Part number - Manufacturer (not distributor) - Part Description (please include meaningful detail) - FSC - Procurement Specification - Comments and clarifications, as appropriate - Estimated quantity required (for procurement forecasting)	

DID 11-4: Project Approved Parts, List

Title: Project Approved Parts List (PAPL)	DID 11-4
Reference: ICESat-2 MAR Paragraph 11.4	
Use: A list of EEE parts that are approved by the Parts Control Board for use in flight hardware.	
Related 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 shall be presented for approval by the PCB	
Preparation Information: The PAPL shall contain all PIL fields plus the following information: - 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 and Data Source - Proton Hardness/Tolerance and Data Source - PMPCB Status - PMPCB Approval Date - PMPCB Required Testing/Evaluations	

DID 11-5: AS DESIGNED PARTS LIST

Title: As Designed Parts List (ADPL)	DID 11-5
Reference: ICESat-2 MAR Paragraph 11.5	
Use: A list of EEE parts that are designed into in flight hardware.	
Related 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 shall be presented for approval by the PCB	
Preparation Information: The As Designed Parts List (ADPL) shall contain all PAPL fields plus the following information: - Assembly Name/Number - Next Level of Assembly - Need Quantity - Reference Designator(s) - Item number (if applicable)	

DID 11-6: AS BUILT PARTS LIST

Title: As Built Parts List (ABPL)	DID 11-6
Reference: ICESat-2 MAR Paragraph 11.6	
Use: A list of EEE parts that are used in the flight hardware.	
Related 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 shall be reviewed by the PCB	
Preparation Information: The As Built Parts List (ABPL): shall contain all ADPL fields plus the following minimum information: - Assembly serial number - Next Level of Assembly serial number - Lot/Date/Batch/Heat/Manufacturing Code, as applicable - Manufacturer's Cage Code (specific plant location preferred) - Distributor/supplier, if applicable - Part serial number (if applicable)	

DID 11-7: BATTERY FOD MITIGATION PLAN

Title: Battery FOD Mitigation Plan	DID 11-7
Reference: ICESat-2 MAR Paragraph 11.8	
Use: Documents what precautions will be done to reduce short circuit events associated with FOD, which may result in loss of the battery.	
Related Documents: Mission Assurance Requirements Document	
Place/Time/Purpose of Delivery: - Delivered to the Project Office thirty 30 days before PDR for review (Preliminary) - Delivered to the Project Office thirty 30 days before CDR for approval (Final)	
Preparation Information: The Battery FOD mitigation plan should include the following: - A description of how FOD is prevented from entering the cell or being generated in the cell (ie: cell assembly in a clean room, cleaning/training frequency, cleaning/brushing and/or inspection of plates/windings, handling of plates/windings, etc.) - A description of how FOD is detected (ie: radiography such as CT scan, electrical characterization, sample cells DPA'ed, etc). - A description of what steps are taken should a cell be suspected of having FOD or other reject cells (ie: radiography, electrical characterization, DPA, etc). - A description of how these reports are shared and used within manufacturing and engineering to prevent future issues and to improve production.	

DID 12-1 MATERIALS AND PROCESSES SELECTION, CONTROL & IMPLEMENTATION PLAN

Title:	DID 12-1
Materials and Processes Selection, Control & Implementation Plan	
Reference:	
ICESat-2 MAR Paragraph 12.0	
Use:	
Defines the implementation of NASA-STD-6016 with the prescribed changes as defined in "Preparation Information" section below.	
Related 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 prescribed changes, described 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 prescribed changes and describe 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 (including MUA/MIUL/Etc. process)
- 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 the requirements in NASA-STD-6016.

- In addition to the requirements of paragraph 4.2.2.11, the developer shall implement a lead-free control plan (LFCP) per GEIA-STD-0005-1 and a tin whisker control plan per Level 2C requirements of GEIA-STD-0005-2 for the use of solders or surface finishes that are less than 3% lead by weight.
- In paragraph 4.1.2, the developer may use GFSC forms or the developer's equivalent forms in lieu of the MAPTIS format.
-

DID 12-2 Life Test Plan for Lubricated Mechanisms

Title: Life Test Plan for Lubricated Mechanisms	DID 12-2
Reference: ICESat-2 MAR Paragraph 12.1	
Use: Defines the life test evaluation process, acceptance criteria, and reporting for lubricated mechanisms.	
Related 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 12-3 MATERIALS USAGE AGREEMENT

Title: Materials Usage Agreement (MUA)	DID 12-3
Reference: ICESat-2 MAR Paragraph 12.2	
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.	
Related 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 MUAs to the Project thirty (30) days prior to PDR for approval - After PDR provide new MUAs to the Project thirty (30) days prior to CDR or before for review - After the initial submission of MUAs, new or 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 12-1). 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 12-4 MATERIALS IDENTIFICATION AND USAGE LIST

Title: Materials Identification and Usage List (MIUL)	DID 12-4
Reference: ICESat-2 MAR Paragraph 12.3	
Use: Establishes the Materials Identification and Usage List (MIUL).	
Related 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 and approval - Provide to the Project Office thirty (30) days prior to CDR for review and approval. - Provide updates to the Project Office within thirty (30) days of identification for review and approval	
Preparation Information: The delivered MIUL shall identify applicable data per NASA-STD-6016 for each material or process listed/proposed.	

DID 12-5 NONDESTRUCTIVE EVALUATION PLAN

Title: Nondestructive Evaluation Plan	DID 12-5
Reference: ICESat-2 MAR Paragraph 12.4	
Use: Establishes the Non-Destructive Evaluation (NDE) plan for the procedures and specifications employed in the inspection of materials.	
Related 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 Facture-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, Standard NDE Guidelines and Requirements for Fracture Control Programs, 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 12-6 PRINTED WIRING BOARDS TEST COUPONS

Title: Printed Wiring Board (PWB) Test Coupons	DID 12-6
Reference: ICESat-2 MAR Paragraph 12.5	
Use: PWB test coupons are evaluated to validate that PWBs are suitable for use in space flight and mission critical ground applications.	
Related 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) - IPC-6018 Microwave End Product Board Inspection and Test - IPC A-600 Guidelines for Acceptability of Printed Boards (Class 3 Requirements)	
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 - In the case that a GSFC-approved laboratory is used, the developer shall deliver the laboratory results to GSFC with the end item data package	
Preparation Information: Notify GSFC regarding shipment of PWB test coupons.	

DID 13-1 ORBITAL DEBRIS ASSESSMENT

Title: Orbital Debris Assessment	DID 13-1
Reference: ICESat-2 MAR Paragraph 13.1	
Use: Ensure NASA requirements for post mission orbital debris control are met.	
Related Documents: - NPR 8715.6A NASA Procedural Requirements for Limiting Orbital Debris - NASA-STD-8719.14 Process for Limiting Orbital Debris	
Place/Time/Purpose of Delivery: - Deliver preliminary assessment to the Project Office fifteen (15) days prior to mission PDR for review - Deliver final package to the Project Office sixty (60) days prior to mission CDR for approval - Deliver updates the final package to the Project Office within thirty (30) days of identification of design changes that affect the assessment for approval	
Preparation Information: The assessment shall be done in accordance with NPR 8715.6 NASA Procedural Requirements for Limiting Orbital Debris and NASA-STD-8719.14 Process for Limiting Orbital Debris. The preliminary assessment is conducted to identify areas where the project may contribute debris and to assess this contribution relative to the guidelines. The final assessment is conducted shall include comments on changes made since the preliminary assessment. The detail should be consistent with the available information of design and operations. The developer shall submit updates to the final assessment for design changes after CDR that impact the potential for debris generation. 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 14-1 GIDEP ALERT / NASA ADVISORY DISPOSITIONS

Title: GIDEP Alert / NASA Advisory Dispositions	DID 14-1
Reference: ICESat-2 MAR Paragraph 14.3	
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 used in NASA product	
Related 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 or material for review - Provide disposition of subsequent Alerts to the Project Office regarding EEE parts or materials already approved for use within 30 days for review	
Preparation Information: The developer shall submit: - A list in accordance with the requirements of the appropriate DID of Paragraph 3.6 and Paragraph 3.7 with a notation for each line item as to whether there are applicable Alerts. - The lists submitted per Paragraph 3.6 and Paragraph 4.3 shall be updated with Alert information as parts and materials are added. - GSFC Form 4-37, "Problem Impact Statement Parts, Materials and Safety" or equivalent developer form, for Alerts provided by the GSFC Project Office.	

DID 14-2 SIGNIFICANT PARTS, MATERIALS, AND SAFETY PROBLEMS

Title: Significant parts, materials, and safety problems	DID 14-2
Reference: ICESat-2 MAR Paragraph 14.3	
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.	
Related 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 15-1 END ITEM ACCEPTANCE DATA PACKAGE

Title: End Item Acceptance Data Package	DID 15-1
Reference: ICESat-2 MAR Paragraph 15.1	
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.	
Related 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, etc.).
- Appropriate approval signatures (e.g., developer's quality representative, product design lead, government Representative, etc.)
- List of shortages or open items at the time of acceptance with supporting rationale.
- As-built serialization (electronic format)
- As-built configuration (electronic format)
- In-process Work Orders (available for review at developers--not a deliverable)
- Final assembly and test Work Order
- Nonconformance reports (electronic format)
- Acceptance testing procedures and report(s), including environmental testing
- Trend data
- Anomaly/problem failure reports with data delineated in DID 2-4 in a comma separated values or comparable electronic format
- Operations Manuals
- 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 were signed by management

APPENDIX D: APPLICABLE DOCUMENTS

Applicable Documents **Applicable Document Name**	**Document Number, Revision, & Date**	**MAR Section(s) and//or DID(s)**	**Document Sources and/or Notes to User**
Quality Management Systems - Requirements	SAE 9100 ,2004	2.1; DID 2-1	http://www.sae.org/standardsdev/
Guidelines for Quality Management System Documentation	ISO/TR 10013:2001 2001	DID 2-1	Purchase at http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fTR+10013%3a2001&source=google&adgroup=iso10&keyword=iso%2Ftr%2010013&gclid=COH58eKq7ZoCFQOcFQodsErqAw .
Launch Range Safety Requirements	No Information	3.1	These documents are mission-specific. Obtain them from the Project Office.
Range Safety User Requirements Manual	AFSPCMAN 91-710, July 2004	3.1.1; DIDs 3-1 through 3-4, DIDs 3-7 through 3-10	http://kscsma.ksc.nasa.gov/ELVPayloadSafety/Requirements.html
Applied Engineering and Technology Directorate Safety Manual Safety Manual	GSFC 500-PG-8715.1.2, Initial, February 23, 2006	3.1.2; DIDs 3-2, 3-5	http://gdms.gsfc.nasa.gov/gdmsnew/home.jsp or Available at RSDO Website, http://rsdo.gsfc.nasa.gov/.
KSC Safety Practices Procedural Requirements	KNPR 8715.3, Revision G, November 12, 2008	3 1. 3.2, DID 3-2, & 3-10	http://kscsma.ksc.nasa.gov/ELVPayloadSafety/Requirements.html
KSC Ionizing Radiation Protection Program	KNPR 1860.1, Revision Basic-1, October 15, 2004	DID 3-15	Available at RSDO Website, http://rsdo.gsfc.nasa.gov/.
Non-Ionizing Radiation Protection Program	KNPR 1860.2, Revision Basic-1, October 15, 2004	DID 3-15	Available at RSDO Website, http://rsdo.gsfc.nasa.gov/.
Standard for Lifting Devices and Equipment	NASA-STD-8719.9, Initial, October 1, 2007	3.4, DIDs 3-5, 6-1	http://www.hq.nasa.gov/office/codeq/doctree/87199.htm
Process for Limiting Orbital Debris	NASA-STD-8719.14, Initial with Change 1, August 28, 2007	3.1.1, 3.2.7; DID 3-11	http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm

Applicable Documents **Applicable Document Name**	**Document Number, Revision, & Date**	**MAR Section(s) and//or DID(s)**	**Document Sources and/or Notes to User**
NASA Procedural Requirements for Limiting Orbital Debris	NPR 8715.6A, Revision A, February 19, 2008	DID 3-11	http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm
NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping	NPR 8621.1, Revision B, May 23, 2006	3.4.8; DID 3-12	http://nodis3.gsfc.nasa.gov/displayDi cfm?Internal_ID=N_PR_8621_001B_&page_nam e=main http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm
Expendable Launch Vehicle Payload Safety Program	NPR 8715.7	3.1, 3.1.1; DID 3-1	http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8715&s=7 http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm
Safety Standard for Explosives, Propellants, and Pyrotechnics	NSS 1740.12, Initial, August 1993	3.1.1	http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm
NASA General Safety Program Requirements	NPR 8715.3 Revision C with Change 3, March 12, 2008	3.1.1, 4.2; DIDs 3-1, 3-4, 3-7, 3-10, 4-1, 4-2& 4-4	http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8715&s=3C http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm
Risk Classification for NASA Payloads	NPR 8705.4, Initial, June 14, 2004	A.1, DIDs 4-1 through 4-4 & 4-6	http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8705&s=4
Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects	NPR 8705.5	4.2; DIDs 4-1 & 4-2	http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8705&s=5
Software Safety Standard	NASA-STD-8719.13, Revision B with Change 1, July 8, 2004	4.2, 5.1	http://www.hq.nasa.gov/office/codeq/doctree/safeheal.htm
NASA Standard for Software Assurance	NASA-STD-8739.8, Initial w/Change 1, July 28, 2004	5.2, DID 5-3	http://www.hq.nasa.gov/office/codeq/doctree/87398.htm http://www.hq.nasa.gov/office/codeq/doctree/87398.pdf

Applicable Documents **Applicable Document Name**	**Document Number, Revision, & Date**	**MAR Section(s) and//or DID(s)**	**Document Sources and/or Notes to User**
NASA Software Engineering Requirements	NPR 7150.2a, Initial, September 27, 2004	5.0, 5.1, DIDs 5-1& 5-2.	http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=7150&s=2
General Environmental Verification Standard (GEVS) for GSFC Flight Programs and Projects	GSFC-STD-7000, Revision D, June 2, 2008	9.0; DIDs 9-1 through 9-6 & 10-2	http://standards.gsfc.nasa.gov/gsfc-stds html http://gdms.gsfc.nasa.gov/gdmsnew/home.jsp (under —Technical Rules||)
For the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)	ANSI/ESD S20.20-2007, March 2007	10.0, 10.2, DID 10-1	http://workmanship nasa.gov/ws_esds2020.jsp http://www.esda.org/keydownloads.html
Guidelines for Acceptability of Printed Boards (Class 3 Requirements)	IPC A-600G, Revision G, September 2004	10.0; DID 12-6	Purchase at http://portal.ipc.org/Association/Index.htm.
Generic Standard on Printed Board Design	IPC-2221A, Revision A, June 2003	10.0	Purchase at http://portal.ipc.org/Association/Index.htm.
Sectional Design Standard for Rigid Organic Printed Boards	IPC-2222, Initial, February 1999	10.0	Purchase at http://portal.ipc.org/Association/Index.htm.
Sectional Design Standard for Flexible Printed Boards	IPC-2223A, Revision A, September 2007	10.0	Purchase at http://portal.ipc.org/Association/Index.htm.
Sectional Design Standard for Organic Multichip Modules (MCM-L) and MCM-L Assemblies	IPC-2225, Initial. March 2000	10.0	Purchase at http://portal.ipc.org/Association/Index.htm.
Generic Performance Specification for Printed Boards (Class 3 Requirements)	IPC-6011, Initial, July 1996	10.0; DID 12-6	Purchase at http://portal.ipc.org/Association/Index.htm.

Applicable Document Name	Document Number, Revision, & Date	MAR Section(s) and//or DID(s)	Document Sources and/or Notes to User
Qualification and Performance Specification for Rigid Printed Boards (Class 3/A Requirements)	IPC-6012B, Revision B with Amendment 1, January 2007	10.0; DID 12-6	Purchase at http://portal.ipc.
Qualification and Performance Specification for Flexible Printed Boards (Class 3 requirements)	IPC-6013B, Revision B, February 2009	10.0; DID 12-6	Purchase at http://portal ipc org/Association/Index.htm.
Qualification and Performance Specification for Organic Multichip Module (MCM-L) Mounting and Interconnecting Structures	IPC-6015, Initial, February 1998	10.0	Purchase at http //portal.ipc.org/Association/Index.htm.
Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies	NASA-STD-8739.1, Revision A March 2008	10.0	http://workmanship.nasa.gov/ws_8739_1.jsp
Workmanship Standard for Surface Mount Technology	NASA-STD-8739.2, Initial with Change 1, June 2008	10.0	http://workmanship.nasa.gov/ws_8739_2.jsp
Soldered Electrical Connections	NASA-STD-8739.3, Initial with Change 3, June 2008	10.0	http://workmanship.nasa.gov/ws_8739_3.jsp http://www.hq.nasa.gov/office/codeq/doctree/87393.htm
Crimping, Interconnecting Cables, Harnesses, and Wiring	NASA-STD-8739.4, Initial with Change 4, July 2008	10.0	http://workmanship.nasa.gov/ws_8739_4.jsp
Fiber Optic Terminations, Cable Assemblies, and Installation	NASA-STD-8739.5. Initial with Change 1, July 2008	10.0	http://workmanship.nasa.gov/ws_8739_5.jsp http://www.hq.nasa.gov/office/codeq/87395.htm
Microwave End Product Board Inspection and Test	IPC-6018A, Revision A, January 2002	10.0, DID 12-6	Purchase at http://portal.ipc.org/Association/Index.htm.
Requirements for the Calibration of Measuring and Test Equipment	ANSI/NCSL Z540.3:2006	10.4.1	Purchase at http://webstore.ansi.org/ or http://store.ncsli.org/Documentary_Standards_C35.cfm.

Applicable Document Name	Document Number, Revision, & Date	MAR Section(s) and/or DID(s)	Document Sources and/or Notes to User
Specification for Destructive Physical Analysis	GSFC S-311-M-70	11.7, DID 11-1	http://nepp.nasa.gov/index_nasa.cfm/472/9252CCDC-CECD-4DD5-A55D4A7080B4F0F1/ Available at RSDO Website, http://rsdo.gsfc.nasa.gov/.
Instructions for EEE Parts Selection, Screening, Qualification, and Derating	GSFC EEE-INST-002 with Addendum 1, April 2008	11.0; DID 11-1	http://nepp.nasa.gov/index_nasa.cfm/477/FFB52B88-36AE-4378-A05B2C084B5EE2CC/ Available at RSDO Website, http://rsdo.gsfc.nasa.gov/
Department of Defense Inspection Program Requirements, Nondestructive for Aircraft and Missile Materials and Parts	MIL-HDBK-6870, Revision A, August 28, 2001	12.4, DID 12-5	http://www.everyspec.com/MIL-HDBK/MIL-HDBK+(3000+-+8999)/MIL-HDBK-6870A_10214/ Note: This is not a Government/Issuing Organization website so documents are not under configuration management.
Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environment	MSFC-STD-3029, Revision A, February 24, 2005	DID 12-3	http://standards.nasa.gov/documents/msfc
Standard Materials and Processes Requirement for Spacecraft	NASA-STD-6016, Initial, July 2008	12.0; DID 12-1 through 12-5	http://standards.nasa.gov/released/NASA/NASA_STD_6016_APPROVED_2008_07_11.pdf
Performance Standard for Aerospace and High Performance Electronics Systems Containing Lead-free Solder	GEIA –STD-0005-1, Revision/Edition 06, June 2006	12.6	Purchase at http://webstore.ansi.org/RecordDetail.aspx?sku=GEIA-STD-0005-1.
Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High Performance Electronic Systems	GEIA-STD-0005-2, Revision/Edition 06, September 4, 2006	12.6	Purchase at http://webstore.ansi.org/RecordDetail.aspx?sku=GEIA-STD-0005-2.
GIDEP Operations Manual	S0300-BT-PRO-010, November 1994	15.1, 15.4; DIDs 15-1 & 15-2	Available at http://www.gidep.org. Note: Various sections/appendices of document were updated between April 1991 and March 2008.