National Aeronautics and
Space Administration

DISC-RQMT-002
REVISION C
June 28, 2013

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

FP21

DISCOVERY PROGRAM SAFETY AND MISSION ASSURANCE GUIDELINES AND REQUIREMENTS

CHECK THE MASTER LIST—
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

Prepared by:

Sonja D. Bernier
MSFC Safety and Mission Assurance

6/28/13
Date

Approved by:

William Kahle
Program Integration Manager
Discovery, New Frontiers, and Lunar Quest Programs

6/28/13
Date

Allen Bacskay
Program Manager
Discovery, New Frontiers, and Lunar Quest Programs

6/28/13
Date

Alan Clark
Chief S&MA Officer
Flight Programs and Partnerships Office

6/28/13
Date

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline	-		Initial Release per Directive # DP1-05-0007
Revision	A	April 7, 2006	General – Changed document font format and miscellaneous grammatical changes. Section 2.0 – Updated applicable documents list. Section 6.8.2 – Revised description of parts screening process. Section 8.2 – Revised Software Quality planning guidelines.
Revision	B	June 6, 2008	Alphabetized applicable and reference documents, Added NPR 7120.5D to applicable documents, revised document to be compliant with 7120.5D, updated document and acronym list and changed S&MA lead sig.
Revision	C	June 28, 2013	Updated document list and signature page, added sections 5.18 and 5.19, added the Discovery Program Library link, removed any requirements that are not imposed by S&MA, updated per 7120.5E, acronym list & signatures per Directive # DP1-00-0019

Table of Contents

1.0 Purpose and Scope

1.1 Purpose

This document establishes the Safety and Mission Assurance (S&MA) guidelines and requirements for the Discovery Program as a means to assure the mission success and safety of personnel, payloads, equipment, and facilities.

1.2 Scope

These guidelines and requirements apply to the design, development, manufacturing, test, integration, flight operations, and pre- and post-mission ground operations phases of Discovery missions. All statements in this document that use the verb "shall" are considered as requirements. Statements that use the verb "should" are considered guidelines that should be considered in the development of the Project Safety and Mission Assurance Plan. Each Discovery Mission should address these guidelines and requirements in their Project Safety and Mission Assurance Plan (this plan may be included as part of the overall Project Plan). EEE parts WCA, and Materials and Processes will be within the Discovery Program Office's responsibility and performed by the MSFC Chief Engineer's Office.

1.3 Applicability

This document is applicable to all Discovery projects. It is recognized that the scope and complexity of Discovery Projects covers a wide range, and tailoring of this document's requirements may be appropriate in some cases. Any requests for proposed tailoring of this document's requirements shall be submitted to the Discovery Program Manager for consideration. Projects that reside at institutions that currently have a NASA-approved S&MA program may utilize their own institutional practices in lieu of this document.

2.0 Documents

2.1 Applicable Documents

DISC-PLAN-001	Discovery Program Plan
NASA-STD-8739.8	Software Assurance Standard
NASA-STD-8719.24	NASA Expendable Launch Vehicle Payload Safety Requirements
NASA/TP-2003-212242	EEE-INST-002: Instructions for EEE Parts Selection, Screening, Qualification, and Derating
NPR 8715.6	NASA Procedural Requirements for Limiting Orbital Debris
NPR 7120.5	NASA Space Flight Program and Project Management Requirements
NPR 8621.1	NASA Procedural Requirements for Mishap Reporting,

	Investigating, and Recordkeeping
NPR 8705.4	Risk Classification of NASA Payloads
NPR 8715.3	NASA General Safety Program Requirements
NPR 8705.6	Safety and Mission Assurance Audits, reviews and Assessments
NPD 8720.1	NASA Reliability and Maintainability (R&M) Program Policy
NPR 8715.7	NASA Expendable Launch Vehicle Payload Safety Requirements
NPR 7123.1A	NASA Systems Engineering Processes and Requirements
SAE AS9100B	Quality Management Systems – Aerospace- Requirements- Technically Equivalent to AECMA prEN 9100

2.2 Reference Documents

2.2.1 NASA Documents

MSFC-STD-2594	MSFC Threaded Fastener Management and Control Practices
NASA -STD- 8719.13	Software Safety Standard
NASA-HDBK-8719.14	Handbook for Limiting Orbital Debris
NASA-STD-8719.14	Process for Limiting Orbital Debris

NASA-STD-8729.1	Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program
NASA-STD-8739.1	Workmanship Standard for Polymeric Application on Electronic Assemblies
NASA-STD-8739.2	Workmanship Standard for 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
NPD 1280.1	NASA Management System Policy
NPD 8700.1	NASA Policy for Safety and Mission Success
NPD 8700.3	Safety and Mission Assurance (SMA) Policy for NASA Spacecraft, Instruments, and Launch Services
NPR 8705.5	Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
NASA/TP-2003-212242	EEE-INST-002: Instructions for EEE Parts Selection, Screening, Qualification, and Derating
NPD 8730.1	Metrology and Calibration
NPD 8730.5	NASA Quality Assurance Program Policy
NPR 7150.2	NASA Software Engineering Requirements
NPR 8735.1	Procedure for Exchanging Parts, Materials, and Safety Problem Data Utilizing the Government Industry Data Exchange Program (GIDEP) and NASA Advisories
OSMA-SMARR-05-01	S&MA Readiness Review

2.2.2 Other Documents

IEEE 730	Standard for Software Quality Assurance Plans—IEEE Computer Society Document

IPC 6011	Generic Performance Specification for Printed Boards
IPC 6012B	Qualification and Performance Specification for Rigid Printed Boards—Incorporating Amendment 1:2007
IPC-2221A	Generic Standard on Printed Board Design
IPC-J-STD-001CD	Requirements for Soldered Electrical and Electronic Assemblies
MIL-STD-1686C	Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)
NASA Pub 1124	Outgassing Data for Selected Spacecraft Materials
	Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, August 2002, http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf
NUREG 0492	Fault Tree Handbook
	Recommended Supplier Surveillance Practices and Independent Verification for Reaction Wheel Procurements – Aerospace Corporation

3.0 Safety & Mission Assurance (S&MA) System and Processes

3.1 S&MA Processes

NPR 8705.4, Risk Classification of NASA Payloads, establishes risk classification levels and provides recommended S&MA requirements for each risk classification level. Historically, the Discovery missions have been Category 2 missions with payloads having a risk classification of B. However, missions using nuclear power sources are Category 1 missions. Mission category levels are defined in NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

Discovery Mission of Opportunity Payloads may have a risk classification less than B. The Discovery projects shall meet the requirements in Appendix B of NPR 8705.4. The proceeding requirements and guidelines in this document provide details on meeting the S&MA aspects of NPR 8705.4 for a risk classification B payload. Mission of Opportunity payloads may require less stringent S&MA requirements, if they are determined to warrant a risk classification of C or D. Any deviations from the requirements in this document shall be approved by the Discovery Program Office as defined in the DISC-PLAN-001, Discovery Program Plan.

3.2 S&MA Planning

The Project Manager (or designee) with assistance from the Safety and Mission Assurance organization should develop a comprehensive Safety and Mission Assurance Plan. The S&MA Plan is developed early in project formulation and addresses S&MA philosophy, organization, approach and all related processes and activities needed for program and occupational safety and mission success. Key Processes include identifying, addressing, and resolving safety and mission success concerns; identifying, mitigating, and accepting risks. Also, the NASA Lessons Learned System (http://llis.nasa.gov/) provides a library of experience that projects can use as reference for best practices, to avoid the repetition of past failures and mishaps, and to prioritize S&MA and Engineering resources.

3.3 Project Reviews

The project should conduct technical reviews by a competent and independent assessment team or teams of experts, to assure that satisfactory progress is being made toward meeting project requirements. These reviews will provide the mechanism to assess performance, assure managerial confidence, enforce technical and programmatic discipline, and convey requirements and progress towards meeting project goals and objectives. The Project S&MA roles and responsibilities for project reviews shall be documented in the Project S&MA Plan.

3.3.1 System Reviews

The Discovery Projects should hold system level reviews as defined in Table 2 of the Discovery Program Plan. The Discovery Project S&MA organizations should participate in the System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), System Integration Review (SIR), Test Readiness Reviews (TRR), Pre-ship/Operational Readiness Review (PSR/ORR), Safety Mission Success Review (SMSR), and Flight Readiness Review (FRR). If the Project's approved Project Plan defines system reviews different than the reviews defined in the Discovery Program Plan, Discovery Project S&MA organizations should participate in those reviews. The scope and function of these reviews are defined in NPR 7123.1A, NASA Systems Engineering Processes and Requirements.

Safety Mission Success Review (SMSR): SMSRs are conducted prior to launch or other mission –critical events/activities by the Chief Safety and Mission Assurance (S&MA) Officer and Chief Engineer (CE) (or senior Center-based S&MA and engineering officials) to prepare for S&MA and engineering participation in critical program/project reviews/decision forums. The S&MA lead and CE lead are the focal points for planning, coordination, and providing the program/project elements of these reviews. Preparation requirements and details for the SMSR process are provided in OSMA-SMARR-05-01 that is entitled S&MA Readiness Review.

3.3.2 Phase E Reviews

During Phase E of a project, the project implements the Missions Operations Plan developed in Pre-Phase A, Phase A, Phase B, Phase C, and Phase D. Phase E is the Operations and Sustainment Life Cycle of the project. The start of Phase E marks the transition from system development and acquisition activities to primarily systems operations and sustainment activities. These activities are focused towards Post Launch Assessment Review (PLAR), Critical Event Readiness Review (CERR), and Post Flight Assessment Review (PFAR). The Safety and Mission Success Review (SMSR), Launch Readiness Review (LRR) and Flight Readiness Review (FRR) process culminates in Key Decision Point (KDP) F. During Phase E, a baseline Systems Decommissioning/Disposal Plan is prepared and documented. The scope and function of these reviews are defined in NPR 7123.1A, NASA Systems Engineering Processes and Requirements.

4.0 System and Industrial Safety

The project shall have a safety program that meets the intent of the requirements that are specified in the NASA General Safety Program Requirements, NPR 8715.3. Safety program responsibility starts at the top with senior management's role of developing policies and providing strategies and resources and is executed by the immediate task supervisor and line organization. All employees are responsible for their own safety, as well as that of others whom their actions may affect. Employees are empowered to call for the halt of any process or operation they believe is unsafe and request analysis by a qualified individual. If the activity is deemed unsafe, the qualified individual will determine the corrective actions needed. Employees are also to report any systems designs, operations, processes, or software they feel are unsafe or do not meet safety requirements.

The project safety organization should be placed at a high enough level and the program implementation authority is vested in a person sufficiently senior to manage the effort so the safety review function can be conducted independently.

Policies, plans, procedures, and standards that define the parameters of the safety program are established, documented, maintained, communicated, and implemented to provide for the appropriate or adequate protection and prevention of loss and damage to personnel, property, material, equipment, and facilities of NASA, other agencies, and the public.

4.1 System Safety

4.1.1 Objective

The principal objective of a system safety activity is to provide for an organized, disciplined approach to the early identification and resolution of hazards impacting personnel, hardware, or mission success to a level as low as reasonably achievable. The project shall identify and document the system safety and mission success risks (hazards) early in the program and continue to update the status of these risks and any newly identified risks throughout the program or project.

All NASA Expendable Launch Vehicle (ELV) Payloads shall meet the requirements specified in NASA-STD-8719.24, NASA Expendable Launch Vehicle Payload Safety Requirements. The payload safety policy is to protect people and resources (including flight hardware and facilities) from hazards associated with ELV payloads and hazard associated with payload to launch vehicle integration, multiple payloads, and payload-related GSE by eliminating the hazards or reducing the risk associated with each hazard to an acceptable level.

4.1.2 Hazard Reduction Protocol

Hazards shall be mitigated according to the following stated order of precedence:

- Eliminate hazards.
- Design for minimum hazards.
- Incorporate safety devices.
- Provide caution and warning devices.

Develop administrative procedures and training.

4.1.3 Hazard Assessment

The hazard assessment process is a principal factor in the understanding and management of technical risk. Hazards are identified and resultant risks are assessed by considering probability of occurrence and severity of consequence. Risk may be assessed qualitatively or quantitatively. System safety is an integral part of the overall program risk management decision process.

4.1.4 System Safety and Mission Success Hazard Analyses

System safety analyses provide a means to systematically and objectively identify hazards, determine their risk level, and suggest the mechanism for their elimination or control. This iterative process begins in the conceptual phase and extends throughout the life cycle including disposal.

There are several types of analyses necessary to identify all the hazards, some of which are specialized and others which, as designs mature, build on previously accomplished analyses.

The first safety analysis is the Preliminary Hazard Analysis (PHA), which should be performed early. Other primary analyses typically include the Subsystem Hazard Analysis (SSHA), Component Level Fault Tree Analysis (FTA), Software Hazard Analysis (SWHA) (see NASA Standard 8719.13, "Software Safety Standard," for more information), System Hazard Analysis

(SHA), Operating and Support Hazard Analysis (O&SHA), Job Hazard Analysis (JHA), Human Factors Engineering Analysis, the Safety Requirements Compliance Matrix, and Integrated Hazard Analysis (IHA), unless otherwise indicated by the PHA. The scope of the safety analyses and the submittal dates shall be documented in the S&MA Plan. Safety analysis is typically provided at design and safety reviews and finalized prior to the FRR. Data from these analyses can be used to offer recommendations to reduce risks.

4.1.5 System Safety and Mission Success Program Reviews

The project manager or his designated agent should conduct one or more system safety and mission success reviews depending on the complexity of the system. These reviews may be in conjunction with other program milestones. The purpose of these reviews is to evaluate the status of hazard analyses, residual risks, hazard controls, verification techniques technical safety requirements, and program implementation throughout all the phases of the system life cycle. These reviews should focus on the evaluation of management and technical documentation and the safety residual risks remaining in the program at that stage of development. Typically, the documentation requirements and the frequencies of reviews are dictated by the vehicle and launch site. If a project's spacecraft contains nuclear materials, it shall provide the required documentation and participate in the Nuclear Launch Safety Approval Process as described in the NPR 8715.3, NASA General Safety Program Requirements.

In accordance with the roles and responsibilities specified in NPR 8715.7, the Payload Manager and Payload Safety Working Group (PSWG) Chairperson are responsible for ensuring that the payload safety review and approval activities take place. Three Safety Reviews shall be completed according to NPR 8715.7. Safety Review I is submitted prior to PDR and to be completed no later than 60 days after the project's PDR. Safety Review II is submitted prior to the project's CDR and to be completed no later than 60 days after the project's CDR. Safety Review III is submitted at least five business days prior to the Launch Services Program's Ground Operations Review which is held before the Payload Projects' Pre-Ship Review.

4.1.6 Mishap Reporting

The objective of mishap and close call investigations is to improve safety by identifying what happened, where it happened, when it happened, why it happened, and what should be done to prevent recurrence and reduce the number and severity of mishaps. The project manager shall meet the procedural requirements specified in NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping.

4.1.7 Orbital Debris

According to NASA's Procedural Requirement for Limiting Orbital Debris, NPR 8715.6, a formal orbital debris assessment should be conducted in accordance with NASA-HDBK 8719.14 or NASA-STD 8719.14 on each space project to determine its potential to generate orbital debris during nominal operations. Also, the design for safe disposal of spacecraft and launch vehicles at the end mission shall be in accordance with NASA-HDBK 8719.14 . Orbital debris is defined as: (1) spacecraft that can no longer perform their mission, (2) rocket bodies, payload adapters or other hardware left on orbit as a result of normal operational activities and (3) fragmentation products from failures or collisions.

Three Orbital Debris Assessment Reports (ODAR) should be completed according to NPR 8715.6. The PDR Draft ODAR is submitted prior to PDR the CDR Draft ODAR is submitted 45 days prior to CDR and the Final ODAR is submitted prior to the beginning of the launch approval process. NASA-HDBK 8719.14 provides the specific information that should be included in a debris assessment.

4.1.8 Telemetry

Telemetry coverage is required during all mission critical events to assure data is available for critical anomaly investigations to prevent future recurrence per NPR 8705.4. Risk Classification for NASA Payloads. Mission critical events in the operation of a spacecraft are those which, if not executed successfully (or recovered from quickly in the event of a problem), can lead to loss or significant degradation of mission. Included in critical event planning are timelines allowing for problem identification, generation of recovery commands, and up linking in a timely manner to minimize risk to the in-space assets.

4.1.9 Meteoroid Environment

Meteroids are defined as naturally occurring free flying space objects and are generally a result of collisions between asteroidal objects or released from comets. There are no specific requirements on spacecraft design and operations, but it is required that spaceflight managers consider the Meteoroid Environment (ME). Per 8715.3, NASA General Safety Program Requirements, the NASA ME Program's objective is to understand the flux of meteoroids which may impact spacecraft traveling in and beyond Earth's orbit. Having knowledge of the meteoroid environment can help spacecraft designers to better protect critical components on spacecraft or avoid critical operations during periods of higher flux.

5.0 Reliability and Maintainability

The Project shall plan and implement an appropriate reliability/maintainability program. Program/Project disciplines, including systems engineering, and hardware design should include effective manufacturing and assembly process controls, effective testing/qualification, product assurance and reliability and maintainability (R&M) engineering as an integral part of the design process. This section explains many of the requirements for a major program. Smaller projects may choose to tailor these requirements to their individual needs. Any deviations to the requirements shall be addressed in the Reliability/Maintainability section of the S&MA Plan.

Note that NASA- preferred Reliability and Maintainability practices can be found at http://www.hq.nasa.gov/office/codeq/rm/prefprac.htm.

5.1 Reliabililty Analysis Requirements

Analyses of hardware design should be performed to ensure proper designed-in reliability and consistency with mission requirements and objectives. The analyses should be performed concurrently with the design effort. Reliability analysis is typically provided at design reviews and finalized prior to FRR. Additional details of each type of required reliability analysis are provided in section 6.3. The required analyses shall be documented in the project S&MA Plan, remain updated through the project life cycle, and shall include the following analyses as a minimum:

Failure Modes and Effects Analysis (FMEA)

- At the assembly level interfaces
- At GSE interfaces
- System FMEA as a minimum down to the circuit block diagram or black box level for class B payloads

Worst Case Analysis (WCA)

- On all parts and circuits

Fault Tree Analysis (FTA)

- Qualitative FTA at a system level

Probabilistic Risk Assessment (PRA)

- As a minimum, a limited scope focusing on mission related end states of specific decision making interest for class B payloads.

5.2 Critical Single Point Failures (SPF)

For class B payloads, critical SPFs for Level 1 requirements are permitted; but are minimized and mitigated by the use of high reliability parts and additional testing. Essential spacecraft functions and key instruments should be fully redundant as practicality permits. Other hardware will have partial redundancy and/or provisions for graceful degradation.

5.3 Reliability Analysis

5.3.1 Failure Modes and Effects Analysis (FMEA)

The main objective of a FMEA is to identify SPFs and to verify that failures will not propagate and damage other hardware. The FMEA should be performed and documented to analyze postulated failures and identify the potential resultant effects. The FMEA should as a minimum:

For interface FMEA:

- Be performed at the assembly level interface to a component level to verify that a failure at the assembly interface circuit cannot propagate to and damage the interfacing circuit

For the System FMEA:

- Consider all operational modes
- Verify that a failure in a system element will be detected and determine the system reaction to the failure.
- Verify that a failure in a non-critical circuit will not affect the performance of a critical circuit.

5.3.2 Electrical/Electronic Worst Case Analysis (WCA)

A WCA should be documented for all circuit designs to demonstrate that sufficient operating margins exist for all operating conditions and performance requirements considering the combination of the following:

- Part temperature range, based on those stated in the environmental requirements. If the thermal analysis indicates a part temperature outside of the specified range, the WCA must be amended to take into account the thermal analysis predicted temperatures.
- Piece part initial tolerance
- Part aging for the operating life of the mission including ground testing time
- Radiation effects
- Special factors such as shock, vibration, or vacuum where such conditions would contribute to variations in the circuit parameters, voltage, frequency, and load variations should also be included.

The analysis should be at least a 3-sigma worst case analysis (i.e. extreme value or extreme value with temperature tracking) in that the value for each of the variable parameters shall be set to limits that will drive the output to a maximum (or minimum) and shall consider Alternate Current (AC), Direct Current (DC) and transient condition effects on the circuit. Piece part parameter data should be obtained from test and/or the appropriate procurement documentation.

Analysis of protective circuitry should be performed to ensure proper operation if a fault were to occur under worst case conditions.

Electrical noise on power lines, including ground differences, and interface signal lines should be considered. Power supply turn on and off transients should be included.

The documentation of the WCAs should describe all identifiable deficiencies and performance restrictions.

5.3.3 Fault Tree Analysis (FTA)

The FTA is a technique that provides a rigorous evaluation of specific undesired events. It is a type of logic tree that is developed by deductive logic from a top undesired event to all sub-events that must occur to cause it. It is primarily used as a qualitative technique for studying undesired events in systems, subsystems, components, or operations involving command paths. The FTA can be used to verify that the FMEA has identified all Critical Single Point Failures (CSPFs) consistent with the top event hazardous condition. It also can be used for quantitatively evaluating the probability of the top event and all sub-event occurrences when sufficient and accurate data are available. The individual failure paths or minimal cut sets should be generated and evaluated for acceptable risk. NUREG 0492 is an excellent reference that may be used in applying the fault tree analysis process.

5.3.4 Probabilistic Risk Assessment (PRA)

PRA characterizes risk in terms of three basic questions: (1) What can go wrong? (2) How likely is it? (3) What are the consequences? The PRA process answers these questions by systematically postulating and quantifying undesired scenarios in a highly integrated fashion. The process uses a collection of models based on systems engineering, probability theory, reliability engineering, physical, and biological sciences, and decision theory.

A "limited-scope" PRA applies the same general rigor as a full-scope PRA but focuses on some of the mission-related end states of specific decision-making interest, instead of all applicable end states.

The process and techniques provided in the NPR 8705.5 and the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners should be used for conducting PRAs. In addition, the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners cites references that provide more detailed information concerning the PRA process.

5.4 Maintainability

Maintainability is a measure of the ease and rapidity with which equipment can be restored to operational status following a failure. Since Discovery Projects are unmanned, all maintainability evaluations will be made on pre-launch operations. The project shall use maintainability analysis to enable system design for accessibility, testability, and ease of inspection. Human factors aspects should also be considered when performing a maintainability analysis. The Project should establish a maintenance concept early in the system development and ensure that compatibility is sustained among system design, maintenance planning, and logistics support activities.

Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program, NASA-STD-8729.1, provides a good discussion of the concepts and the formulation of maintainability into a project. It should also consider providing a built-in test capability that provides an on-board, automated test capability to detect, diagnose, isolate, and recover from system failures.

5.5 Limited Life Items

Limited life items are defined as those items that have a limited useful life due to deterioration associated with either the passage of time; or accumulation of mate and de-mate, and operating time cycles. Limited life items require periodic replacement or refurbishment to assure that operating characteristics have not degraded beyond acceptable limits. Shelf life and storage requirements for limited life items shall be identified and controlled.

5.6 Government Industry Data Exchange Program (GIDEP) Acute Launch Emergency Reliability Tip (ALERT)

ALERT System documentation provides information relative to unexpected failures or discrepant conditions of parts and materials used in equipment which may be of significant application in other equipment and to safety problems of general concern. This applies to failures or discrepant conditions encountered when such parts or materials are applied within the limits of the applicable specification.

The Project Team shall have access to and maintain knowledge of parts problems as reported in the Government Industry Data Exchange Program (GIDEP). Any provided NASA ALERTs shall be reviewed, evaluated and, if found applicable, documented justification for continued use or implementation of appropriate countermeasures will be provided. Parts subject to ALERT reviews include flight hardware, ground support equipment, and test equipment.

5.7 Closed Loop Problem/Failure Reporting

A closed loop problem/failure reporting and corrective action system shall be established to support hardware and software problem detection and assessment, and hardware repair. This system will allow the developer to implement design improvements and corrections as a part of the design process. The data collected will support tracking the root cause of the problem. Failure reporting and corrective action shall be continued through Phase E of the project.

5.8 Electrical, Electronic and Electromechanical (EEE) Parts

5.8.1 General Requirements

Discovery projects shall implement a parts program that assures mission reliability and performance requirements are met for the expected mission life. The Project Team should control the management, selection, application, evaluation, and acceptance of all parts through a Parts Control Board.

All EEE parts shall meet NASA/TP-2003-212242 Level 2, Level 2 equivalent Source Control Drawings (SCDs), and/or requirements per NASA Center Parts Management Plan. Other parts selection or screening methods that meet or exceed the intent of the NASA requirements may be used if approved by the Parts Control Board.

System design and EEE parts selection should be such that their intended application shall be met in the predicted mission radiation environment. The resulting design should be latch-up immune and should minimize single event upsets.

5.8.2 Flight Parts Screening

Screening testing should be done to the requirements of the most applicable military specification for the part type and any additional tests needed to meet the application requirements. In addition to the parts level screening tests, component or system level tests demonstrate the reliability of the parts and their assemblies. These tests should be performed no matter what grade of parts is used in the development of the hardware. However, the results of these tests do not improve the reliability of the individual parts, and cannot, for example, be used to assume the same reliability for a commercial part as for a level 2 part.

5.8.3 De-rating

The de-rating of parts improves the reliability of systems. All EEE parts shall be used in accordance with the de-rating guidelines of the NASA/TP-2003-212242 EEE-INST-002 Level 2 for class B payloads, for applicable devices or an equivalent that is approved by the Parts Control Board.

5.8.4 Radiation Hardness

Parts should be selected to meet their mission application in the predicted radiation environment. The radiation environment consists of two separate concerns, total dose, and single event effects.

5.8.4.1 Total Dose

Total dose radiation may damage semiconductor devices and microcircuits either by displacement (lattice damage by recoil) or ionization (electron-hole pair generation). In bipolar devices displacement and ionization cause gain degradation and an increase in leakage currents. Total dose damage is cumulative and is a function of time, exposure, and shielding. As time of exposure increases and shielding decreases the absorbed total dose will increase.

5.8.4.2 Single Event Effects (SEE)

Single Event Effects (SEE) is phenomena, affecting integrated circuits or power transistors caused by a single high-energy particle strike. These events may cause either "soft" errors or "hard" errors.

A "soft" error or Single Event Upset (SEU) occurs when the logic state of a circuit is changed. It can be corrected by reloading the correct information into memory or by restarting an algorithm.

A "hard" error results in permanent damage to a device and can cause circuit failure. Examples of "hard" errors include Single Event Gate Rupture (SEGR) in N-channel power transistors, Single Event Burnout (SEB) in power transistors and Single Event Latch up (SEL) in complementary metal-oxide-semiconductor (CMOS) integrated circuits.

5.8.4.3 Parts Storage Control

Parts shall be stored in a controlled environment that protects the parts from excessive temperatures and humidity and from contamination. An electrostatic discharge (ESD) control plan shall be implemented for ESD sensitive parts. Traceability by part number, manufacturer, and lot date code should be maintained for parts in controlled storage.

5.8.4.4 Parts Identification List

A Parts Identification List (PIL) shall be prepared, maintained, and updated by the project in accordance with the project's configuration control system. The PIL should be compiled by experiment component, instrument, or instrument component and should include as a minimum the following information: part number, part name or description, manufacturer name or Commercial and Government Entity (CAGE) number, quantity, and drawing number and name of the next higher assembly where part is located. The part number should be the military specification part number if it is a military part or the manufacturer's part number if it is a commercial part.

The developer should maintain traceability by part number, manufacturer, and lot date code for all EEE parts assembled into flight hardware through the use of configuration identification lists (build paper).

5.9 Materials and Processes

Discovery Projects shall implement a Materials and Processes program. NASA Reference Publication 1124 entitled "Outgassing Data for Selecting Spacecraft Materials" should be used as a guide for materials selection.
Discovery projects should identify contamination requirements and establish and maintain a contamination control program consistent with mission requirements.

Fastener selection and use shall be controlled. MSFC-STD-2594C should be used as a guide.

Each Discovery project shall maintain a list of materials (polymeric, composites, and inorganic), lubricants, processes and appropriate usage records prior to and during the hardware development and the as built list should be available for review at the Pre-ship Review.

6.0 Quality Assurance

6.1 Scope

The Discovery Projects shall define and implement a quality system that meets the intent of SAE AS9100B. This section defines the detailed quality assurance (QA) activities to be implemented during the formulation, design, build, assemble, and test phases of the Discovery projects. It encompasses all program flight, non-flight, test and ground support hardware and software.

6.2 Initial Quality Planning

6.2.1 Review of Project Documents

Quality planning should begin with participation by Quality Assurance personnel in the review and generation of inputs to the governing project requirement documents.

6.2.2 Workmanship

The Discovery project shall impose workmanship standards which help assure that the required mission lifetime and performance are met. The following commercial or NASA workmanship standards are given as guidelines and should be considered for use:

> Soldered Electrical Connections: NASA Technical Standard NASA-STD-8739.3, Soldered Electrical Connections or IPC-J-STD-001CD, Requirements for Soldered Electrical and Electronics Assemblies
>
> Cabling, Harnessing and Crimping: NASA Technical Standard NASA-STD-8739.4, Crimping, Interconnecting Cables, Harnesses, and Wiring
>
> Conformal Coating and Staking: NASA-STD-8739.1, Workmanship Standard for Polymeric Application on Electronic Assemblies.

ESD Controls: MIL-STD-1686, Electrostatic Discharge Control Program for Protection of Electrical and Electronics Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)

Surface Mount Technology (SMT): NASA-STD-8739.2, Workmanship Standard for Surface Mount Technology

Printed Wiring Board Design: IPC-2221A, Generic Standard on Printed Board Design

Printed Wiring Board Procurement: IPC 6011 AND IPC 6012B, Class 3/A

Fiber Optic: NASA Technical Standard NASA-STD-8739.5, Fiber Optic Terminations, Cable Assemblies, and Installation.

Additional NASA Voluntary Consensus Standards are found at http://workmanship.nasa.gov/wkstds_vcs.jsp. Use of other workmanship standards is permitted if they meet or exceed the NASA standards for the given application. The rationale for meet or exceed application is provided at the system reviews. Concurrence for use should be coordinated as early as possible.

6.2.3 Pre-Procurement Activity

The Office of Quality Assurance should support the implementation of the procurement phase by participation in the following areas of activity:

- Review procurement documentation, including Requests for Proposals (RFPs), Statements-Of-Work (SOWs), Procurement Requisitions, and Equipment Specifications to ensure appropriate quality provisions and clauses are defined, including Contractor End-Item-Data-Package requirements. Recommended practices for inserting quality statements into purchase orders or contract "terms and conditions" (often referred to a "quality clauses" for contracts) have been developed for use as a best practices approach and can be found at http://www.hq.nasa.gov/office/codeq/quality/qa_clause/frameset.htm. The available statements have been developed to reduce confusion and uncertainty associated with quality requirement flow down within the aerospace industry. The statements should be considered on a case-by-case basis and applied where appropriate as an alternate to one-off phraseology intended to convey the same meaning.

- Provide the technical divisions and the procurement divisions with information concerning contractor quality system capabilities derived from previous and current quality efforts.

- Ensure contractor Quality Plan compliance to procurement requirements.

- Perform vendor audits at potential suppliers. Scheduled audits, and random, unscheduled audits, should be performed in order to effectively assess existing conditions and operations. For scheduled audits, provisions should exist to ensure that each quality area is audited. The results of audits in each area should be documented in a report with requests for correction of deficiencies. Management action should be taken to ensure effective correction of the reported deficiencies. Follow up reviews should be made to ensure that required corrections have been implemented.

6.3 Design and Development Control

Quality Assurance personnel should participate in preliminary and critical design reviews, pre-environmental test reviews, hardware certification reviews and/or pre-shipment acceptance reviews. Personnel responsible for quality comments and recommendations should be formally documented.

Quality Assurance personnel should review and approve (signature block on drawings) Top Assembly and Mechanical Interface Control Documents (MICDs).

6.3.1 Training and Certification

Personnel performing hands on fabrication, assembly, and inspection of flight hardware shall be trained and certified to NASA requirements defined in section 6.2.2, or contractor equivalent document. Quality Assurance should verify that all certifications are current and valid.

6.4 Change Controls

Change control shall be accomplished in accordance with the applicable Project Configuration Management Plan. Unless otherwise specified by the contract, the Project Change Control requirements should be flowed down to sub-contractors. Quality assurance should participate in change control by:

- Reviewing and approving all drawing changes.
- Reviewing software system requirement changes after initial baseline is completed.
- Maintaining master red-line drawing sets, when necessary.
- Verifying all approved changes are properly incorporated/implemented.
- Verifying product as-built configuration.

6.5 Procurement Controls

When parts or materials have their inspectable attributes covered and cannot be adequately inspected at the projects facility, or when they are determined to be critical processes for high-risk items, source inspection should be performed at the supplier's facility. Records of inspection and tests performed at source should be maintained as part of the Hardware End Item Data Package (EIDP), Acceptance Data Package or an equivalent document.

6.5.1 Raw Material Controls

Suppliers of raw materials should supply certifications indicating that materials being provided are in compliance with the requirements of the procurement documents. Reports of tests required determining conformance to applicable specifications and drawings are required when requested by the hardware engineer or quality engineer, and should be included as required deliverable documentation.

When necessary, these reports are verified by source inspection or by independent tests performed in addition to the supplier reports. When raw material is found to be non-compliant, it shall be tagged and segregated from acceptable material. An Inspection Report should be generated and dispositioned prior to the material being released.

6.6 Receiving Inspection

Receiving inspection shall be performed on all flight-received materials and hardware to ensure that procured hardware is compliant.

Quality Assurance responsibilities during receiving inspection should include the following:

- Inspection of incoming hardware for compliance to applicable drawings, specifications, and/or other documentation specified by the contract or purchase order.
- Documenting, segregating, and obtaining disposition of non-conforming hardware and/or material.
- Maintaining a system to control the use and accuracy of all tools, gauges, jigs, and fixtures used for the inspection and acceptance of mechanical hardware.
- Generating the necessary documentation required to certify hardware acceptance.

6.7 Processing, Fabricating, Assembly, Test, and Inspection Control

Flight hardware or material shall have documented evidence of Quality Assurance acceptance. Preliminary Material Review Board action or project waiver shall be required for nonconforming hardware or material. All processes used in the fabrication of flight hardware shall be qualified in accordance with NASA requirements defined in section 6.2.2 or contractor equivalent requirements.

6.7.1 Inspection

All protoflight and flight hardware shall be inspected to release drawings, specifications, and approve workmanship standards, unless otherwise specified by Project documentation. Unreleased documents should be documented on an Electronic Inspection Report or contractor equivalent. Redlined documents, if permitted by the Project, shall be maintained in accordance with the Project Configuration Management Plan.

Mechanical flight hardware should have 100% dimensional inspections performed unless otherwise specified in the Project S&MA Plan.

All reduced inspection programs should be approved by the project Quality Assurance Representative. Hardware subjected to a reduced inspection program without the written approval of the Project QA Representative shall be considered non-compliant, and documented on an Electronic Inspection Report, or contractor equivalent.

All protoflight and flight hardware and materials should be inspected at the level necessary to:

- Assure workstations and areas in which protoflight or flight hardware is present meet the Electrostatic Discharge (ESD) requirements as defined by the Project.
- Assure the Project Configuration Management Plan and hardware traceability requirements are met.
- Assure training and certification requirements are compliant.
- Assure workmanship, fit, form, and function compliance.
- Any electrical interfaces and requirements are compliant.
- Assure applicable handling, packaging, and storage requirements are documented and complied with.
- Assure applicable handling and operating constraints have been identified and adhered to.
- Assure that flight hardware documentation accompanies the flight hardware during any transportation activities.

Precap inspections should be performed on all hybrid microcircuits, Application-Specific Integrated Circuits (ASICs), and nonstandard relays.

6.7.2 Stamp Controls

Inspection stamps on the applicable documentation that accompanies the hardware indicate inspection status of hardware. Quality Assurance Stamp Control shall be maintained by the Project's Quality Assurance Records Center or equivalent.

6.7.3 Metrology controls

All electrical, electronic, linear, mechanical, optical, temperature and vacuum/pressure equipment used to determine or verify product conformance/acceptability shall be subject to calibration/certification. All equipment shall be within the valid calibration period at the time it is used for determination of product conformance/acceptability. All test equipment calibration on Discovery Projects shall be controlled in accordance with projects quality plan.

6.7.4 Controlled Storage

Flight hardware shall be maintained in controlled storage areas. The storage areas should have the necessary environmental and ESD controls required to meet project requirements. Access shall be controlled and limited to those persons involved in fabrication, test, and quality assurance tasks.

6.7.5 Non-conforming Material Control

A closed-loop system for identifying documenting, controlling, and correcting nonconformances shall be implemented. When an article or material does not conform to applicable engineering design documentation such as drawings or specifications, it shall be identified as non-conforming, segregated from acceptable articles (to the degree practicable), held for further action and the nonconformance documented. At contractors, nonconformances should be documented on Inspection Report or equivalent forms. Each nonconformance should be reviewed, dispositioned, and corrective and preventative action taken to prevent recurrence of similar discrepancies.

Project Quality Assurance personnel should maintain status of all nonconformances.

6.7.6 Material Review Board (MRB)

Provisions for documenting, disposition, and mitigating major and minor nonconformances should be included in Project Quality Assurance section of S&MA Plans and/or the contract Statement of Work by instituting a Material Review Board. Project Quality Assurance personnel should ensure effective corrective and preventative actions are implemented.

6.7.7 Acceptance Test Verification

Quality Assurance should support the implementation of functional acceptance and environmental test programs. The following specific Quality Assurance activities should be implemented to verify that testing is performed in compliance with the established project test program requirements.

6.7.7.1 Preparation of Test Procedures/Specifications

Quality Assurance should verify that:

- The detail test procedures identify the applicable project test requirements.
- All applicable specifications and procedures have been properly authorized prior to use, and all deviations/waivers from the specifications and procedures are authorized.

6.7.7.2 Environmental Testing

Quality Assurance should monitor flight hardware environmental testing performed and should ensure that:

- The test area is controlled to the extent necessary to protect the test article from damage or degradation.
- Requirements governing safety, handling, and storage, calibration, cleanliness and environmental controls are being adhered to.
- Test equipment and support instrumentation are within current calibration cycles.
- Fixture evaluations, as evidenced by documentation, meet the requirements of the applicable specifications.
- That test readiness review checklists have been completed, if required, and all action items have been closed or dispositioned "OK to proceed."
- Facility, Operational, and ESD Surveys have been completed.
- Problem Failure Reports (PFRs) or the contractor equivalent of both forms, are initiated when required and within the required time frame.

6.7.7.3 Functional and Acceptance Electrical Testing

Quality Assurance should monitor flight hardware functional and electrical acceptance testing performed at all levels of assembly and should ensure that:

- Authorized test procedure is available and in use.
- Test data and acceptance criteria are documented.
- Test equipment is within its current calibration cycle.

- Safety, hardware handling, and required storage provisions are in effect.
- ESD precautions are being adhered to.
- The test area is controlled to the extent necessary to protect the hardware and personnel safely.
- Contamination control and environmental control requirements are being adhered to.
- Procedural and specification changes are properly documented.
- Problem/Failure Reports are initiated for any noted test anomalies, when required.

6.7.7.4 Post-Test Hardware Inspection

Post-Test Hardware Inspections should be performed to detect and document the condition of the hardware after environmental testing, with emphasis on documenting discrepancies that may have resulted from the testing.

6.8 Ground Support Equipment

Quality Assurance involvement in Ground Support Equipment (GSE) is typically limited to the level necessary to assure:

- Flight Hardware interfaces, mechanical and/or electrical are compliant to requirements
- Current calibration of Electrical GSE
- Current proof-load of Mechanical GSE
- Cleanliness and contamination control requirements are compliant
- Proper and legible identification of the product
- Safety requirements are satisfied and potential hazards are identified

6.9 End Item Acceptance Data

Hardware fabricated, assembled, and/or tested or procured from a contractor should have a data package that contains pedigree sufficient enough to validate the hardware as spaceflight worthy. End Item Acceptance Data Package requirements are called out in the Project Configuration Management or Documentation Plans. Contractor End Item Data Package and as-built requirements are defined in the contract Statement-of-Work, in the Contract CDRLs/DRDs, or on the purchase orders. The minimum End Item Acceptance Data should include, but not be limited to:

- As-built data as defined by the Project Configuration Management Plan.
- A complete listing of any open or unapproved documentation (such as Problem/Failure Reports, Inspection Reports, MRBs, etc.).
- Final Acceptance Test Data.
- Handling and Operating Constraints as defined by the Critical Item Transportation Plan.
- Telemetry calibration data, if applicable
- Limited Life Data (such as shelf life, cycle life, etc.)
- Contractor Certificate of Compliance
- Operation and Maintenance Manuals
- Listing of any ship short items

- Requirements Compliance Verification Matrix

6.10 Hardware Functional and Physical Configuration Audit (FCA/PCA) Reviews

If Hardware Functional and Physical Configuration Audit (FCA/PCA) Reviews or equivalent are specified in the configuration management or the project plan, Quality Assurance personnel should participate in and support. The Project Manager or their designee should determine project hardware that requires FCA/PCA. Specifically, Quality Assurance personnel should be responsible for the accomplishment of the following:

- Assure submittal to the Hardware Functional and Physical Configuration (FCA/PCA) Board of supporting data that reflects the complete quality history of the hardware, which includes inspection status, configuration verification, and Material Review Board (MRB) activities.
- Assure identification to the Hardware FCA/PCA Board of any and all discrepancies that arise from incomplete certification and/or deliverable documentation requirements.
- Identification of any waivers, deviations, or exceptions to established project requirements.
- Indication, by signature, on the Hardware FCA/PCA Review that the hardware meets the applicable requirements and a satisfactory certification has been obtained.
- Assure an Inspection Report has been generated which denotes inspection acceptance of the hardware or identifies any discrepancies and their dispositions.

6.11 Launch Operations Support

Project Quality Assurance should provide the necessary support to ensure a correct and safe integration of Project deliverables with the Launch Vehicle. Quality Assurance activities should include, but not be limited to:

- Inspect prior to shipment that includes verification of compliance with the Packaging, Handling, and Transportation Record, or equivalent information.
- Post-transportation inspection.
- Surveillance and monitoring to assure compliance to Spacecraft processing and testing procedures.
- Performing and documenting necessary inspections.
- Verification of completion of all required hardware and software integration testing.
- Verification of compliance to procedures and requirements regarding Spacecraft/Payload in preparation for Launch Vehicle integration.
- Participation in Launch Vehicle Integration Readiness Reviews.
- Ensure Program Handling constraints are clearly identified and complied with in integration procedures.
- Monitoring and ensuring Spacecraft/Payload contamination control procedures are followed.

6.12 Operations Personnel Training and Certification

The Project organization shall impose training and certification standards that help assure the required mission lifetime and science performance are met. Training requirements should take into account all project unique considerations such as preparations for encounter, impact, or sample return, and re-certification after hibernation. The Project Training organization should maintain the necessary training and certification records to ensure operations personnel have received the appropriate training and verify all certifications are current and valid.

7.0 Software Assurance

A Software Assurance (SA) program shall be established in accordance with the Software Assurance Standard NASA-STD-8739.8 or another standard of equal or greater measure. Compliance with the Standard will assure conformance of a given software system to established requirements, development methodologies, and standards.

Software assurance is the planned and systematic set of activities that ensures that software processes and products conform to requirements, standards, and procedures. It includes the disciplines of Software Quality (functions of Software Quality Engineering, Software Quality Assurance (SQA), and Software Quality Control), Software Safety, Software Reliability, Software Verification and Validation, and Independent Verification and Validation (IV&V). 'Processes' include all of the activities involved in concept formulation, specifying, designing, developing, enhancing, and maintaining software; 'products' include the software, associated data, its documentation, and all supporting and reporting paperwork.

7.1 Software Assurance Program Requirements and Guidelines

This SA program shall be in effect throughout the life of the project, beginning with requirements definition and continuing into the sustaining engineering phase. The SA program should be coordinated with the hardware and system assurance programs established to meet the rest of the requirements of this document. The following items should be addressed during the establishment of the software assurance program.

- The Discovery Projects should plan, document, and implement a software assurance program for software development, operation, and maintenance activities. This includes documentation of software assurance procedures, processes, tools, techniques, and methods to be used.
- The software assurance program should include processes for assurance of commercial off-the-shelf (COTS), military off-the-shelf (MOTS), and government off- the-shelf (GOTS) software addressing both the basic acquired software and any modifications or applications written to adopt them into the intended system.
- The software assurance program should include the disciplines of Software Quality, Software Safety, Software Reliability, and Software Verification and Validation.
- When Independent Verification and Validation has been selected for a project, the provider should coordinate with IV&V personnel to share data and information.

7.2 Software Assurance Plan

The Discovery Projects shall establish and maintain a software assurance plan that addresses all software development and maintenance activities.

The software assurance plan should:

- Conform to IEEE 730, Standard for Software Quality Assurance Plans.
- Address how the Discovery Projects will implement the requirements of NASA-STD-8739.8.
- If there is any conflict between the NASA-STD-8739.8 and IEEE 730, Standard for Software Quality Assurance Plans, NASA-STD-8739.8 shall take precedence.

APPENDIX A Acronyms

AC	Alternate Current
ADP	Acceptance Data Package
AFSPC MAN	Air Force Space Command Manual
ALARA	As Low As Reasonably Achievable
ALERT	Acute Launch Emergency Reliability Tip
ASIC	Application-Specific Integrated Circuit
CAGE	Commercial and Government Entity
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CE	Chief Engineer
CM	Configuration Management
CMOS	Complementary Metal Oxide Semiconductor
COTS	Commercial Off-the-Shelf
CSPFs	Critical Single Point Failures
DC	Direct Current
DNFLQP	Discovery, New Frontiers, and Lunar Quest Programs
DRD	Data Requirements Document
EEE	Electrical, Electronic and Electromechanical
EIDP	End Item Data Package
EOMP	End of Mission Plan
ERRIC	Electronics Radiation Response Information Center
ESD	Electrostatic Discharge
FCA/PCA	Functional/Physical Configuration Audit
FRR	Flight Readiness Review
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
GIDEP	Government Industry Data Exchange Program
GSE	Ground Support Equipment
GOTS	Government Off-the-Shelf
IEEE	Institute of Electrical and Electronics Engineers
IHA	Integrated Hazard Analysis
IV & V	Independent Verification and Validation
JHA	Job Hazard Analysis
JPL	Jet Propulsion Laboratory
MICD	Mechanical Interface Control Document/Drawing
MDR	Mission Design Review
MOS	Metal Oxide Semiconductor
MOTS	Military Off-the-Shelf
MRB	Material Review Board
MRR	Mission Readiness Review
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements

NSS	NASA Safety Standards
O&SHA	Operating and Support Hazard Analysis
ODAR	Orbital Debris Assessment Report
OSMA	Office of Safety and Mission Assurance
PDR	Preliminary Design Review
PER	Pre-Environmental Review
PFR	Problem Failure Report
PHA	Preliminary Hazard Analysis
PIL	Parts Identification List
PRA	Probabilistic Risk Assessment
PSR/ORR	Pre-Ship Review/Operational Readiness Review
PSWG	Payload Safety Working Group
QA	Quality Assurance
R&M	Reliability and Maintainability
RADNET	Radiation Effects Database
RDD	Release Description Document
RFP	Requests for Proposal
SA	Software Assurance
S& MA	Safety and Mission Assurance
SCDs	Source Control Drawings
SDLC	Software Development Life Cycle
SEB	Single Event Burnout
SEE	Single Event Effects
SEGR	Single Event Gate Rupture
SEL	Single Event Latch up
SEU	Single Event Upset
SHA	System Hazard Analysis
SMARR	Safety and Mission Assurance Readiness Review
SMSR	Safety Mission Success Review
SMT	Surface Mount Technology
SOW	Statement of Work
SPFs	Single Point Failures
SQA	Software Quality Assurance
SRCR	Software Review Certification Requirement Review
SRR	System Requirements Review
SSHA	Subsystem Hazard Analysis
STD	Standard
SWHA	Software Hazard Analysis

APPENDIX B Requirement Table

The table below contains each requirement by section number:

Section	Requirement
3.1	The Discovery projects shall meet the requirements in Appendix B of NPR 8705.4. Any deviations from the requirements in this document shall be approved by the Discovery Program Office.
3.2	The Project Manager (or designee) with assistance from the Safety and Mission Assurance organization shall develop a comprehensive Safety and Mission Assurance Plan.
3.3	The project shall conduct technical reviews by a competent and independent assessment team or teams of experts, to assure that satisfactory progress is being made toward meeting project requirements.
3.3.1	The Discovery Projects should hold system level reviews as defined in Table 2 of the Discovery Program Plan.
4.0	The project shall have a safety program that meets the intent of the requirements that are specified in the NASA General Safety Program Requirements, NPR 8715.3.
4.1.1	The project shall identify and document the system safety and mission success risks (hazards) early in the program and continue to update the status of these risks and any newly identified risks throughout the program or project. All NASA Expendable Launch Vehicle (ELV) Payloads shall meet the requirements specified in NASA-STD-8719.24, NASA Expendable Launch Vehicle Payload Safety Requirements.
4.1.5	If a project's spacecraft contains nuclear materials, it shall provide the required documentation and participate in the Nuclear Launch Safety Approval Process as described in the NASA General Safety Program Requirements. In accordance with the roles and responsibilities specified in NPR 8715.7, the Payload Manager and Payload Safety Working Group (PSWG) Chairperson are responsible for ensuring that the payload safety review and approval activities take place. Three Safety Reviews shall be completed according to NPR 8715.7.
4.1.6	The project manager shall meet the procedural requirements specified in NPR 8621.1 NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping.
4.1.7	Per NPD 8715.6, a formal orbital debris assessment should be conducted in accordance with NASA-STD 8719.14 on each space project to determine its potential to generate orbital debris during nominal operations.
4.1.8	Telemetry coverage is required during all mission critical events to assure data is available for critical anomaly investigations to prevent future recurrence per NPR 8705.4. Risk Classification for NASA Payloads.

4.1.9	Per 8715.3, NASA General Safety Program Requirements, the NASA ME Program's objective is to understand the flux of meteoroids which may impact spacecraft traveling in and beyond Earth's orbit.
5.0	The required analyses shall be documented in the project S&MA Plan, remain updated through the project life cycle, and shall include the following analyses as a minimum:
5.1	Failure Modes and Effects Analysis: • At the assembly level interfaces • At GSE interfaces • System FMEA as a minimum down to the circuit block diagram or black box level for class B payloads Worst Case Analysis • On all parts and circuits Fault Tree Analysis • Qualitative FTA at a system level Probabilistic Risk Assessment • As a minimum, limited scope focusing on mission related end states of specific decision making interest for class B payloads
5.5	Shelf life and storage requirements for limited life items shall be identified and controlled.
5.5.1	The Project Team shall have access to and maintain knowledge of parts problems as reported in the Government Industry Data Exchange Program (GIDEP). Any provided NASA ALERTS shall be reviewed, evaluated and, if found applicable, documented justification for continued use or implementation of appropriate countermeasures will be provided.
5.6	A closed loop problem/failure reporting and corrective action system shall be established to support problem detection and assessment, and hardware repair.
5.8.1	Discovery projects shall implement a parts program that assures mission reliability and performance requirements are met for the expected mission life. All EEE parts shall meet NASA/TP-2003-212242 Level 2, Level 2 equivalent Source Control Drawings, and/or requirements per NASA Center Parts Management Plan. Other parts selection or screening methods that meet or exceed the intent of the NASA requirements may be used if approved by the Parts Control Board.
5.8.3	All EEE parts shall be used in accordance with the de-rating guidelines of the NASA/TP-2003-212242 Level 2 for class B payloads, for applicable devices or an equivalent that is approved by the Parts Control Board.
5.8.4.3	Parts shall be stored in a controlled environment that protects the parts from excessive temperatures and humidity and from contamination. A Parts Identification List (PIL) shall be prepared, maintained, and updated by

	the project in accordance with the project's configuration control system.
5.8.4.4	Discovery Projects shall implement a Materials and Processes program.
	Fastener selection and use shall be controlled.
5.9	Each Discovery project shall maintain a list of materials (polymeric, composites, and inorganic), lubricants, processes and appropriate usage records prior to and during the hardware development and the as built list should be available for review at the Pre-ship Review.
6.1	The Discovery Projects shall define and implement a quality system that meets the intent of SAE AS9100.
6.2.2	The Discovery project shall impose workmanship standards which help assure that the required mission lifetime and performance are met.
6.3.1	Personnel performing hands on fabrication, assembly, and inspection of flight hardware shall be trained and certified to NASA requirements defined in section 7.2.2, or contractor equivalent document.
6.4	Change control shall be accomplished in accordance with the applicable Project Configuration Management Plan.
6.5.1	Suppliers of raw materials shall supply certifications indicating that materials being provided are in compliance with the requirements of the procurement documents.
	When raw material is found to be non-compliant, it shall be tagged and segregated from acceptable material.
6.6	Receiving inspection shall be performed on all flight-received materials and hardware to ensure that procured hardware is compliant.
6.7	Flight hardware or material shall have documented evidence of Quality Assurance acceptance. Preliminary Material Review Board action or project waiver shall be required for nonconforming hardware or material. All processes used in the fabrication of flight hardware shall be qualified in accordance with NASA requirements defined in section 7.2.2 or contractor equivalent requirements.
6.7.1	All protoflight and flight hardware shall be inspected to release drawings, specifications, and approved workmanship standards, unless otherwise specified by Project documentation. Redlined documents, if permitted by the Project, shall be maintained in accordance with the Project Configuration Management Plan.
6.7.2	Quality Assurance Stamp Control shall be maintained by the Project's Quality Assurance Records Center, or equivalent.
6.7.3	All equipment shall be within the valid calibration period at the time it is used for determination of product conformance/acceptability. All test equipment calibration on Discovery Projects shall be controlled in accordance with projects quality plan.
6.7.4	Flight hardware shall be maintained in controlled storage areas. Access shall be controlled and limited to those persons involved in fabrication, test, and quality

	assurance tasks.
6.7.5	A closed-loop system for identifying documenting, controlling, and correcting nonconformances shall be implemented. When an article or material does not conform to applicable engineering design documentation such as drawings or specifications, it shall be identified as nonconforming, segregated from acceptable articles (to the degree practicable), held for further action and the nonconformance documented.
6.12	The Project organization shall impose training and certification standards that help assure the required mission lifetime and science performance are met. Training requirements should take into account all project unique considerations such as preparations for encounter, impact, or sample return, and re-certification after hibernation. The Project Training organization should maintain the necessary training and certification records to ensure operations personnel have received the appropriate training and verify all certifications are current and valid.
7.0	A Software Assurance (SA) program shall be established in accordance with the Software Assurance Standard, NASA-STD-8739.8, or another standard of equal or greater measure.
7.1	This SA program shall be in effect throughout the life of the project, beginning with requirements definition and continuing into the sustaining engineering phase.
7.2	The Discovery Projects shall establish and maintain a software assurance plan that addresses all software development and maintenance activities.