Subject: Risk Classification for NASA Payloads

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Preface

P.1 Purpose

This directive defines (1) the criteria for Mission Directorates to define the risk tolerance classes for NASA missions and instruments, and (2) the corresponding Agency-level assurance expectations that drive design and analysis, test philosophy, and common assurance practices.

P.2 Applicability

a. This directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory (a Federally-Funded Research and Development Center), other contractors, recipients of grants, cooperative agreements, or other agreements only to the extent specified or referenced in the applicable contracts, grants, or agreements.

b. This directive applies to NASA robotic programs and projects, including those flown on human vehicles, managed in accordance with NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

c. This directive does not apply to human vehicles, launch systems, carrier vehicles, or non-spaceflight aeronautical systems (e.g., airplanes). Application of this directive as a result of foreign collaborations to on-orbit services or non-NASA missions provided to NASA is at the discretion of the responsible NASA Mission Directorate. In this NPR, the scope of mission risk classification is understood to be limited to the spacecraft or scientific payloads launched on a transport vehicle.

d. This directive does not apply to projects managed under NPR 7120.8, NASA Research and Technology Program and Project Management Requirements, or projects otherwise not managed under NPR 7120.5, though these projects may choose to impose the objectives from Appendix D in their project-level documentation.

e. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms “may” denotes a discretionary privilege or permission, “can” denotes statements of possibility or capability, “should” denotes a good practice and is recommended, but not required, “will” denotes expected outcome, and “are/is” denotes descriptive material.

f. In this directive, all document citations are assumed to be the latest version unless otherwise noted. Use of more recent versions of cited documents may be authorized by the responsible Safety and Mission Assurance (SMA) Technical Authority (TA).

g. The requirements enumerated in this document are applicable to all new projects managed in accordance with NPR 7120.5 that are in Formulation Phase as of or after the effective date of this document (see NPR 7120.5 for project phase definitions).

P.3 Authority

NPD 8700.1, NASA Policy for Safety and Mission Success.

P.4 Applicable Documents and Forms

NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

P.5 Measurement/Verification

Compliance by programs and projects with the requirements contained within this directive is verified as part of selected life-cycle reviews, and by assessments, reviews, and audits. Compliance with the requirements contained within this directive is also monitored by Centers, Mission Directorates, and by the SMA TA.

P.6 Cancellation

NPR 8705.4, Risk Classification for NASA Payloads, dated June 14, 2004.

Chapter 1. Introduction

1.1 Overview

1.1.1 This directive establishes four risk tolerance classes and the associated expectations corresponding to the acceptable risk and degree of uncertainty that a Mission Directorate assigns to a project.

1.1.2 These four distinct risk tolerance classes provide projects with a uniform authoritative source of Agency-level assurance expectations from which managers, technical authorities, engineers, etc., can develop, communicate, and implement appropriate mission assurance and risk management strategies and requirements consistent with corresponding NASA assurance standards.

1.1.3 This directive also identifies programmatic and institutional SMA directives that do not vary by risk tolerance class and are implemented for each project.

1.2 Delegation of Responsibilities

1.2.1 Unless specifically prohibited, responsibilities and requirements may be delegated. The stated role or actor remains accountable for its implementation and outcome.

1.2.2 Where an office or organization is stated as the actor of a requirement, the Official in Charge of that office or organization is responsible and accountable for the action and its outcome.

1.3 Request for Relief

The process for requesting relief and the granting of waivers from requirements within this directive is defined in NPR 8715.3, NASA General Safety Program Requirements.

Chapter 2. Roles and Responsibilities

2.1 Mission Directorate Associate Administrator

2.1.1 The Mission Directorate Associate Administrator's (MDAA), as stated in NPD 1000.3, The NASA Organization, is responsible for defining, funding, evaluating, advocating, and overseeing the implementation of NASA programs and projects to ensure their outcomes meet schedule and cost constraints as well as performance requirements. As part of this responsibility, the MDAA operating or sponsoring the mission:

a. Implements SMA directives and requirements provided in paragraph 3.3.1.

b. Establishes and documents the risk classification and associated SMA objectives for NASA missions and instruments with support from the Chief, SMA and the Chief Engineer.

> *Note: A constellation of spacecrafts may be treated as one mission with a single risk classification. When individual elements of NASA missions and instruments have distinct mission objectives, the MDAA may designate different risk tolerance classes for the corresponding elements.*

c. Reviews for approval the project's formulation of SMA objectives consistent with the designated risk tolerance class(es).

2.1.2 As specified in NPR 8000.4, programmatic authorities are accountable for risk acceptance decisions for their programs and projects throughout the program and project life-cycle. The MDAA and NASA program offices flow risk acceptance authority down to NASA project offices as defined in their program-level documentation.

2.2 NASA Project Manager

2.2.1 The NASA Project Manager is responsible for:

a. Establishing, documenting, and executing the project's SMA Plan specifying assurance plans, standards, methods, processes, and practices consistent with the mission or instrument risk classification and SMA objectives established by the Mission Directorate.

b. Reporting execution status of the project's detailed implementation of assurance standards, methods, processes, and practices to the Mission Directorate, the Office of Safety and Mission Assurance (OSMA), and the Office of the Chief Engineer (OCE) at all Key Decision Points (KDPs), Life-Cycle Reviews (LCRs), and Safety and Mission Success Review (SMSR).

2.2.2 When the responsible Mission Directorate or NASA program office has not established a NASA project office, any responsibilities or requirements levied on the NASA Project Manager in this directive are reverted to the NASA Program Manager.

2.3 The Chief, Safety and Mission Assurance

2.3.1 The Chief, SMA, as stated in NPD 1000.3 is responsible for advising the Administrator and other senior officials on matters related to risk, safety, and mission success. As part of this responsibility, the Chief, SMA:

a. Supports Mission Directorates in the development and review of risk classification for NASA missions and instruments.

b. Reviews the project's formulation of SMA objectives consistent with the designated risk tolerance class(es).

c. Supports Mission Directorates in the implementation of SMA directives and requirements provided in paragraph 3.3.1.

d. Exercises general oversight and coordinates Agency-wide implementation of this NPR.

2.4 The Chief Engineer

2.4.1 The Chief Engineer, as stated in NPD 1000.3, is responsible for advising the Administrator and other senior officials on matters related to technical readiness in execution of NASA programs and projects. As part of this responsibility, the Chief Engineer:

a. Supports Mission Directorates in the development and review of risk classification for NASA missions and instruments.

b. Reviews the project's formulation of SMA objectives consistent with the designated risk tolerance class(es).

2.5 Project-Level SMA Technical Authority

2.5.1 Project-Level SMA TAs are individuals appointed by the Center SMA Director to exercise the TA role within projects.

2.5.2 The Project-Level SMA TA is responsible for assuring that the formulation and implementation of the project's SMA Plan is technically sound and consistent with established risk classifications and associated SMA objectives.

Chapter 3. Risk Classification Process and Related SMA Implementation

3.1 NASA Mission and Instrument Risk Classification

3.1.1 The MDAA establishes a set of mission directorate requirements reflecting the key objectives of the project for NASA missions and instruments (see NPR 7120.5).

3.1.2 The Mission Directorate designates the mission or instrument risk tolerance class as early in the formulation process as possible (e.g., Announcement of Opportunity (AO)).

3.1.3 The risk tolerance classes, further characterized in Appendix C, are:

3.1.3.1 **Class A:** The lowest risk tolerance that is driven more by technical objectives. This would normally represent a very high priority mission with very high complexity, as described in Appendix C.

3.1.3.2 **Class B:** Low risk tolerance that is driven more by technical objectives. This would normally represent a high priority mission with high complexity, as described in Appendix C.

3.1.3.3 **Class C:** Moderate risk tolerance that is driven more by technical objectives. This would normally represent a medium priority mission with medium complexity, as described in Appendix C.

3.1.3.4 **Class D:** High risk tolerance that is driven more by programmatic constraints. This would normally represent a lower priority mission with a medium to low complexity, as described in Appendix C.

3.1.4 The MDAA shall designate and document mission and instrument risk tolerance classes in the KDP B Decision Memorandum, considering the guidance in Appendix C.

3.1.5 The MDAA may choose to not designate a mission or instrument risk tolerance class or to designate a mission or instrument at a higher risk tolerance than Class D if the Mission Directorate determines that mission or instrument has a higher risk tolerance than the risk tolerance classes described in paragraph 3.1.3.

3.1.5.1 Such missions or instruments still document any SMA objectives in Appendix D imposed on the project by the sponsoring organization (e.g., Request for Proposal, AO) and their approach to satisfy those objectives in an Assurance Implementation Matrix as defined in paragraph 3.2.2.

3.1.5.2 Such missions or instruments are still subject to the requirements listed in paragraph 3.3.1.

3.1.6 The MDAA, in consultation with the Chief, SMA and the Chief Engineer, may change the risk classification for NASA missions and instruments in Formulation Phase (see NPR 7120.5 for project phase definitions).

3.2 Project-Specific Implementation of the Mission or Instrument Risk Classification

3.2.1 Appendix D identifies reference SMA objectives to be satisfied as a function of the designated risk tolerance class. Projects satisfy the objectives in Appendix D either using standards that have already been accepted by NASA and are identified in Appendix D; or using alternate approaches or standards proposed by the project and determined to be appropriate for the mission, risk tolerance class, and specified application by the Technical Authorities. This provides projects with the flexibility to propose tailored and innovative means of meeting the SMA objectives.

3.2.2 Prior to SRR, the Project Manager shall formulate and obtain MDAA approval and Chief, SMA and Chief Engineer concurrence of SMA objectives consistent with the designated risk tolerance class(es) and reference SMA objectives in Appendix D. The objectives should be documented via an Assurance Implementation Matrix (see Appendix E) appended to the (Preliminary) Project Plan (see NPR 7120.5). In lieu of the Assurance Implementation Matrix, the MDAA may invoke a standardized Mission Assurance Requirements document.

> *Note: The Science Mission Directorate (SMD) Standard Mission Assurance Requirements Payload Classification: D is an example of a standardized Mission Assurance Requirements document.*

3.2.3 The NASA Project Manager, with concurrence from the Project-Level SMA TA, shall establish, document, and implement the project's SMA Plan detailing project-specific assurance plans, standards, methods, processes, and practices consistent with the approved Assurance Implementation Matrix.

3.2.4 The NASA Project Manager shall obtain Project-Level SMA TA concurrence on departures from the SMA Plan including standards referenced therein. When appropriate, concurrences are obtained in accordance with Center-level processes to resolve such matters as the tailoring of and waivers and deviations to requirements.

3.2.5 At LCRs, KDPs, and SMSR, the NASA Project Manager shall report actual and planned departures from the baseline Assurance Implementation Matrix to the Mission Directorate and the OSMA.

3.3 General SMA Requirements

3.3.1 The following documents are applicable to NASA missions and instruments regardless of risk tolerance class:

a. NPR 8020.12, Planetary Protection Provisions for Robotic Extraterrestrial Missions.

b. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

c. NPR 8705.6, Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments; Chapter 3. Safety and Mission Success Review (SMSR).

d. NPR 8715.3, NASA General Safety Program Requirements; Chapter 6. Nuclear Safety for Launching of Radioactive Materials.

e. NPR 8715.5, Range Flight Safety Program.

f. NPR 8715.6, NASA Procedural Requirements for Limiting Orbital Debris and Evaluating the Meteoroid and Orbital Debris Environments.

g. NPR 8715.7, Expendable Launch Vehicle (ELV) Payload Safety Program.

h. NPR 8735.1, Exchange of Problem Data Using NASA Advisories and the Government-Industry Data Exchange Program (GIDEP).

3.3.2 Processes for the relief from the requirements in these directives are defined in NPR 8715.3, section 1.13.

3.3.3 Centers and Mission Directorates may develop and update derived policies, standards, and guidelines to expand upon the requirements referenced in the documents and specified sections in paragraph 3.3.1 of this directive for the unique needs of their respective projects. Projects may further be subject to Center-level safety and health requirements.

Appendix A. Definitions

Acceptable Risk. A level of risk, referred to a specific item, system or activity, that, when evaluated with consideration of its associated uncertainty, satisfies pre-established risk criteria.

Breadboard. A low fidelity unit that demonstrates function only, without respect to form or fit. It often uses commercial and/or ad hoc components and is not intended to provide definitive information regarding operational performance.

Concurrence. A documented agreement by a management official that a proposed course of action is acceptable.

Critical Item. A critical item is one which if defective or fails, causes a catastrophic event affecting the public, NASA workforce, high-value assets, or mission success. Reliability considerations apply to determination of criticality for cases where loss of multiple units of the item in question is required for the catastrophic event to be realized, and the units are of the same design and build lot and have a common failure mode relevant to the critical function (e.g., fasteners, capacitors).

Critical Process. A critical process is an activity performed by NASA, suppliers, or NASA services suppliers during mission development, launch preparations, launch, commissioning, operations and decommissioning that if defective or fails to achieve the intended results directly contributes to or causes a catastrophic event affecting the public, NASA workforce, high-value assets, or mission success.

Decision Memorandum. The document that summarizes the decisions made at KDPs or as necessary in between KDPs. The decision memorandum includes the Agency Baseline Commitment (if applicable), Management Agreement cost and schedule, unallocated future expenses, and schedule margin managed above the project, as well as life-cycle cost and schedule estimates, as required.

Engineering Unit. A high fidelity unit that demonstrates critical aspects of the engineering processes involved in the development of the operational unit. Engineering test units are intended to closely resemble the final product (hardware/software) to the maximum extent possible and are built and tested so as to establish confidence that the design will function in the expected environments. In some cases, the engineering unit can become the final product, assuming proper traceability has been exercised over the components and hardware handling.

Fault Tolerance. The built-in ability of a system to provide continued correct operation in the presence of a specified number of faults or failures.

Fault. An undesired system state and/or the immediate cause of failure (e.g., maladjustment, misalignment, defect, or other). The definition of the term “fault” envelopes the word “failure,” since faults include other undesired events such as software anomalies and operational anomalies.

Flight Qualification Unit. Flight hardware that is tested to the levels that demonstrate the desired qualification level margins. Sometimes this means testing to failure. This unit is never used operationally.

Flight Unit. The actual end item that is intended for deployement and operations. It is subjected to formal functional and acceptance testing.

Flight Spare. The spare end item for flight. It is subjected to formal acceptance testing. It is identical to the flight unit.

Graceful Degradation. Ability of a systems or component to work to maintain limited functionality even when a large portion of it has been destroyed or rendered inoperative. The purpose of graceful degradation is to prevent catastrophic failure.

Launch Constraint. Bounding conditions limiting or restricting aspects of launch related operations.

Life-Cycle Cost. The total of the direct, indirect, recurring, nonrecurring, and other related expenses both incurred and estimated to be incurred in the design, development, verification, production, deployment, prime mission operation, maintenance, support, and disposal of a project, including closeout, but not extended operations. The Life-Cycle Cost (LCC) of a project or system can also be defined as the total cost of ownership over the project or system's planned life-cycle from Formulation (excluding Pre-Phase A) through Implementation (excluding extended operations). The LCC includes the cost of the launch vehicle.

Mission. A major activity required to accomplish an Agency goal or to effectively pursue a scientific, technological, or engineering opportunity directly related to an Agency goal. Mission needs are independent of any particular system or technological solution.

Project Plan. The document that establishes the project's baseline for Implementation, signed by the responsible program manager, Center Director, project manager, and the MDAA, if required.

Proof of Concept. Analytical and experimental demonstration of hardware/software concepts that may or may not be incorporated into subsequent development and/or operational units.

Protoflight Unit. Protoflight units are developed for cases when a qualification unit is not developed (due to cost or schedule constraints). The protoflight unit is intended for flight or deployment and operations. A limited set of qualification and tests are performed on the prototype to preserve its ability to function and life expectancy. Full acceptance testing is performed.

Qualification Unit. Hardware that is generated with the same components and processes intended for the actual flight units. These units are tested to the levels that demonstrate the desired qualification level margins of key parameters such as thermal extremes, vibration, and radiation levels. Sometimes this means testing the unit to failure. This unit is not used operationally, but if still functioning, may be kept as a ground spare or test unit for mission anomalies.

Risk. The potential for shortfalls with respect to achieving explicitly established and stated objectives. As applied to programs and projects, these objectives are translated into performance requirements, which may be related to mission execution domains (safety, mission success, cost, and schedule) or institutional support for mission execution. Risk is operationally characterized as a set of triplets:

The scenario(s) leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage).

The likelihood(s) (qualitative or quantitative) of those scenarios.

The consequence(s) (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.

Uncertainties are included in the evaluation of likelihoods and identification of scenarios.

Risk Classification. A stakeholder's declaration of tolerance for risk based on factors such as priority, national significance, technological challenge, and resources available, used to recommend a set of activities and level of scrutiny for maintaining the level of risk.

Risk Tolerance. The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.

Risk Appetite. Amount and type of risk that an organization is willing to pursue or retain.

Single Point Failure. An independent element of a system (hardware, software, or human), the failure of which would result in loss of mission objectives, hardware, or crew as defined for the specific application or project.

Appendix B. Acronyms

AO	Announcement of Opportunity
ARB	Anomaly Review Board
EEE	Electronics, Electrical, and Electromechanical
FAR	Federal Acquisition Regulation
FMEA	Failure Modes and Effects Analysis
FRB	Failure Review Board
IV&V	Independent Verification and Validation
GCQA	Government Contract Quality Assurance
HQ	Headquarters
KDP	Key Decision Point
LCC	Life-Cycle Costs
LCR	Life-Cycle Review
MAR	Mission Assurance Requirements
MDAA	Mission Directorate Associate Administrator
MRB	Material Review Board
M&P	Materials and Processes
NASA-STD	NASA Standard
NFS	NASA FAR Supplement
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OEM	Original Equipment Manufacturer
OSMA	Office of Safety and Mission Assurance
PRR	Production Readiness Review
QA	Quality Assurance

QMS	Quality Management System
R&M	Reliability & Maintainability
SCD	Source Control Drawing
SMA	Safety and Mission Assurance
SMD	Science Mission Directorate
SME	Subject Matter Expert
SMSR	Safety and Mission Success Review
SPF	Single Point Failure
TA	Technical Authority
TRR	Test Readiness Review

Appendix C. Risk Classification Considerations for Class A – Class D NASA Missions and Instruments

C.1 This appendix provides considerations for designating a mission or instrument risk tolerance class. These considerations constitute a structured approach for identifying a hierarchy of risk tolerances commensurate with the four risk tolerance classes defined in Chapter 3.

C.2 The considerations provided are to be treated holistically with each taken into account in order to most appropriately designate a mission or instrument risk tolerance class based on the applicable mission criteria. The considerations provided in the table below are not definitive, nor is any specific mission criterion alone intended to be the ultimate driver to designating a mission or instrument risk tolerance class. Ultimately, the mission or instrument risk tolerance class is designated by the Mission Directorate in accordance with paragraph 3.1.4.

C.3 Other considerations for designating a mission or instrument risk tolerance class may exist that are not explicitly expressed in this appendix (e.g., alternate research or reflight opportunities, launch constraints).

Mission and Instrument Risk Classification Considerations		
Priority (Relevance to Agency Strategic Plan, National Significance, Significance to the Agency and Strategic Partners)	Very High: High: Medium: Low:	Class A Class B Class C Class D
Primary Mission Lifetime	Long, > 5 Years: Medium, 5 Years > – > 3 Years: Short, 3 Years > – > 1Years: Brief, < 1 Year:	Class A Class B Class C Class D
Complexity and Challenges (Interfaces, International Partnerships, Uniqueness of Instruments, Mission Profile, Technologies, Ability to Reservice, Sensitivity to Process Variations)	Very High: High: Medium: Medium to Low:	Class A Class B Class C Class D
Life-Cycle Cost	High : Medium to High Medium : Medium to Low	Class A Class B Class C Class D

Appendix D. Program and Project Safety and Mission Assurance Objectives for Class A – Class D

D.1 Appendix D provides program and project SMA objectives that vary according to risk tolerance class over a continuum of design and management controls, systems engineering processes, mission assurance requirements, and risk management processes to be satisfied in project-specific mission assurance implementation.

D.2 The expectation is that individual projects may mix and match components from different mission or instrument risk tolerance classes to meet the intent of the mission's overall classification and avoid being more or less conservative than the overall risk tolerance class and mission requirements dictate.

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
Fault Tolerance (including SPFs), Reliability, and Maintainability	Establish the reliability, maintenance, maintainability, and fault tolerance philosophy to address mission success and safety, and identify corresponding Reliability and Maintainability (R&M) methods (e.g., FMEA, Fault Tree Analysis, Critical Items List, Critical Item Control Plan) in NASA-STD-8729.1, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systemsand/or alternative standards being used to capture, analyze, mitigate, or control faults and failures, including Single Point Failures (SPFs), in the Assurance Implementation Matrix (See Appendix E). Provide on-going insight and status during subsequent LCR reviews by addressing corresponding risks and associated risk mitigation and contingency plans, as applicable, commensurate with the mission type and mission or instrument risk tolerance class(es). **Accepted Standard:** NPR 7123.1, Appendix G; NASA-STD-8729.1.			
	Fault tolerance and graceful degradation designed and implemented addressing all critical items or processes whose failure would result in failure to meet mission objectives, injury to personnel, or collateral	Fault tolerance and graceful degradation designed and implemented addressing mission success criteria and critical risks where failure would result in injury to personnel or collateral damage.	Fault tolerance and graceful degradation designed and implemented addressing, at the discretion of the Program and Project, mission success criteria. Fault tolerance and graceful	Fault tolerance and graceful degradation designed and implemented for critical risks where failure would result in injury to personnel or collateral damage. Address R&M objectives for

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	damage. Establish R&M requirements and associated analysis and verification methods for all applicable R&M objectives. Formally document assumptions and rationale for any objectives in NASA-STD-8729.1A not being addressed.	Establish R&M requirements and associated analysis and verification methods for all applicable R&M objectives. Formally document assumptions and rationale for any objectives in NASA-STD-8729.1A not being addressed.	degradation designed and implemented addressing critical risks where failure would result in injury to personnel or collaterial damage. Address selected R&M objectives (i.e., requirements and associated analysis and verification methods) for critical items or processes whose failure would result in failure to meet mission objectives. Address R&M objectives (i.e., requirements and associated analysis and verification methods for critical items or proceses where failure would result in injury to personnel oor collateral damage.	critical items or processes whose failure would result in injury to personnel or collateral damage.
Environmental Test Program Verification and Validation	Establish a qualification, flight acceptance, and protoflight test program to verify and validate performance in an operational, simulated operational, or relevant space environment. Include an approach to utilizing breadboards, proof of concept models, engineering units, qualifications units, flight unit, and flight spare units.			
	Complete system verification and validation testing. Qualification and flight	Complete system verification and validation testing. Mixed qualification, flight	Complete system verification and validation testing. Mixed qualification, flight	Complete system verification and validation testing. Mixed qualification, flight

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	acceptance test program for development and flight units. Flight spare units are flight acceptance tested if designated for flight. Protoflight test program for primary and secondary structures is acceptable. End-to-end testing of critical functions using flight software wherever possible; otherwise, use of qualified software simulators.	acceptance, and protoflight test programs for development and flight units. Flight spare units are flight acceptance or protoflight tested if designated for flight. Protoflight test program for primary and secondary structures is acceptable. End-to-end testing of critical functions using flight software wherever possible; otherwise, use of qualified software simulators.	acceptance, and protoflight test programs for development and flight units. Flight spare units are flight acceptance or protoflight tested if designated for flight. Protoflight test program for primary and secondary structures is acceptable. End-to-end testing of critical functions using flight software wherever possible; otherwise, use of qualified software simulators.	acceptance, and protoflight test programs for development and flight units. Flight spare units are flight acceptance or protoflight tested if designated for flight. Testing at higher levels of assembly is acceptable. Protoflight test program for primary and secondary structures is acceptable. Testing at higher levels of assembly including system level is acceptable. End-to-end testing of critical functions using flight software wherever possible; otherwise, use of qualified software simulators.
Electronics, Electrical, and Electromechanical (EEE) Parts	Select EEE parts at an appropriate level for functions tied directly to mission success commensurate with safety, performance and environmental requirements. Perform additional screening and qualification tests, as necessary, to reduce mission risk. For secondary functions not tied directly to mission success, lower level parts are acceptable in accordance with project-level documentation **Accepted Standard:** NASA-STD-8739.10, Electrical, Electronic, and Electromechanical (EEE) Parts Assurance Standard.			
	Level 1 parts, equivalent Source Control Drawings (SCD) or requirements per	Class A criteria or Level 2 parts, equivalent SCD or requirements per Center	Class B criteria or Level 3 parts, equivalent SCD or requirements per Center	Class C criteria or Level 4 parts, equivalent SCD or requirements per Center

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	Center Parts Management Plan.	Parts Management Plan.	Parts Management Plan.	Parts Management Plan.
Materials	Prepare and implement Materials and Processes (M&P) Selection, Control, and Implementation Plan. Implement an M&P Control Board process or similar developer process that defines the planning management, and coordination of the selection, application, procurement, nondestructive evaluation, control, and standardization of M&P and for directing the disposition of M&P problem resolutions. **Accepted Standard:** NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft.			
	Requirements are applicable based on critical items and processes whose failure would result in failure to meet mission objectives, injury to personnel, or collateral damage. Materials assessed for application and life limits.	Requirements are applicable based on critical items and processes whose failure would result in failure to meet mission objectives, injury to personnel, or collateral damage. Materials assessed for application and life limits.	Requirements are applicable based on critical items and processes whose failure would result in failure to meet mission objectives, injury to personnel, or collateral damage. Materials assessed for application and life limits.	Requirements are applicable based on critical items or processes whose failure would result in injury to personnel or collateral damage.
Telemetry Coverage for Critical Events	Monitor and downlink to ground station or relay spacecraft or record telemetry coverage during critical events where failure would result in failure to meet mission objectives. 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. Examples include separation from a launch vehicle, critical propulsion events, deployment of appendages necessary for communication or power generation, stabilization into a controlled power positive attitude, and entry-descent and landing sequences.			
	Monitor and downlink to ground station and record spacecraft telemetry coverage during all events where failure would result in failure to meet mission	Monitor and downlink to ground station and record spacecraft telemetry coverage during all events where failure would result in failure to meet mission	Record telemetry coverage during all events where failure would result in failure to meet mission objectives to assure data are available for critical	Record telemetry coverage during all events where failure would result in failure to meet mission objectives to assure data are available for critical

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	objectives to assure data is available off of the flight system to support mission operations and anomaly investigations to prevent future recurrence.	objectives to assure data is available off of the flight system to support mission operations and anomaly investigations to prevent future recurrence.	anomaly investigations to prevent future recurrence.	anomaly investigations to prevent future recurrence.

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
Quality Assurance and Quality Engineering	Plan, document, and implement the quality assurance plans and quality engineering functions described in NPD 8730.5 and NPR 8735.2, including how the critical design, construction, and verification specifications are captured and conveyed to project SMA teams, system developers, and hardware suppliers; how quality data will be managed; supplier risk management; quality management system elements and elements of production readiness; product and process quality assurance and product acceptance; and how risks due to nonconformance will be managed. **Accepted Standard:** NPD 8730.5, NASA Quality Assurance Program Policy; NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects.			
	Broadly apply quality controls and quality assurance processes throughout the hardware development lifecycle in a manner that defines conformance criteria for all levels of hardware and processes and that produces a continuous record of conformance and traceability to technical specifications and requirements. Require established design and construction technical standards and quality management system standards to minimize supply chain risk and demonstrate adequate production readiness, both	Apply quality controls and quality assurance processes to systems identified as strongly tied to mission success objectives throughout the hardware development lifecycle in a manner that defines conformance criteria and that produces a continuous record of conformance and traceability to technical specifications and requirements. Require established design and construction technical standards and quality management system standards to minimize supply chain risk and demonstrate adequate production readiness, both	Apply quality controls and quality assurance processes to systems identified as strongly tied to mission success objectives throughout the hardware development lifecycle. Require established design and construction technical standards and quality management system standards to minimize supply chain risk and demonstrate adequate production readiness, both for in-house and external supplier hardware production and launch and mission operations functions. Leverage off of industry	Apply quality controls and quality assurance processes to systems identified as tied to safety objectives throughout the hardware development lifecycle. Compare established design and construction technical standards and quality management system standards to suppliers' standards to identify supplier quality risks. Use focused audits and production or test readiness reviews to identify and mitigate production risks. Use insight methods for supplier quality surveillance. Acquire and use quality data and other quality

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	for in-house and external supplier hardware production and launch and mission operations functions. Determine supplier risk using requirement implementation plans and physical audits. Apply design review processes that include evaluations of manufacturability and manufacturing process stability. Use results of oversight as well as insight supplier quality surveillance methods as evidence of compliance for both processes and products. Acquire and use quality data and other quality deliverables to track quality assurance rigor and risks across the entire mission lifecycle. Use review boards and corrective action processes to resolve nonconformances. Build and use product	for in-house and external supplier hardware production and launch and mission operations functions. To determine supplier risk, require prime developer implementation plans and perform physical audits of key or higher risk suppliers. Address manufacturability risks for unique or custom constructions. Apply oversight as well as insight supplier quality surveillance methods for key or high risk processes and products. Acquire and use quality data and other quality deliverables to track quality assurance rigor and risks across the entire mission lifecycle. Use review boards and corrective action processes to resolve nonconformances. Build and use product acceptance data packages that demonstrate	standards for design, construction and verification specifications for custom or unique constructions and processes. Perform assessments of key suppliers and physical audits of higher risk suppliers. Use insight methods for supplier quality surveillance. Acquire and use quality data and other quality deliverables to track quality assurance rigor and risks across the entire mission lifecycle. Use review boards to resolve nonconformances. Build and use product acceptance data packages that record conformance of the product to its key technical specifications.	deliverables to track quality assurance rigor and risks across the entire mission lifecycle. Use review boards to resolve nonconformances. Build and use product acceptance data packages that record conformance of the product to its key technical specifications.

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	acceptance data packages that demonstrate requirements compliance and that substantiate flight readiness.	requirements compliance and that substantiate flight readiness.		

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
Software	Requirements tailoring by Software Classes is provided in NPR 7150.2, Software Engineering Requirements, and Software Assurance tailoring provided by Software Class is provided in NASA-STD-8739.8, Software Assurance Standard. **Accepted Standard:** NPR 7150.2; NASA-STD-8739.8.			
	Flight software is designated as "Software Class B" (see NPR 7150.2). Software Independent Verification and Validation (IV&V) is performed on Category 1 projects, Category 2 projects (see NPR 7120.5), or projects selected explicitly by the Chief, SMA.	Flight software is designated as "Software Class B" (see NPR 7150.2). Software IV&V is performed on Category 1 projects, Category 2 projects (see NPR 7120.5), or projects selected explicitly by the Chief, SMA.	Flight software is designated as "Software Class B" (see NPR 7150.2). Software IV&V is performed on projects selected explicitly by the Chief, SMA.	Flight software is designated as "Software Class C" (see NPR 7150.2). Software IV&V is performed on projects selected explicitly by the Chief, SMA.
Risk Informed Decision Making (RIDM) and Continuous Risk Management (CRM) Processes	Plan, implement, and document a graded approach to Risk Management implementing Risk Informed Decision Making (RIDM) and Continuous Risk Management (CRM) processes as detailed in NPR 8000.4 and NASA/SP-2011-3422. Support risk-informed selection of project and activity solutions and designs by developing, comparing, documenting and communicating to organizational decision-makers the risk profiles of available alternatives and corresponding performance measures. Proactively identify risks using well-structured statements, risk scenarios, decisions (i.e., accept, watch, research, mitigate, elevate, and close risks) based on risk ranking, rationale behind all recommendations to management, and controls. Conduct Analysis of Alternatives (AoA) to develop risk mitigation strategies. Make reassessments of the risk response strategies on a continuous basis. Tracking of individual risks, leading indicators, and performance measures on a continuous basis. Tracking concentrates			

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	on realization and operational stages of the lifecycle. Communicate results, decisions, and associated rationale to programmatic chains of command. Make recommendations on reformulation and reallocation of objectives, requirements, and risk tolerances. **Accepted Standard**: NPR 8000.4, Agency Risk Management Procedural Requirements			
	Apply comprehensive scope and rigor across programmatic, engineering, institutional, partnership, and enterprise domains, addressing mission technical, cost, schedule, safety, and security performance. RIDM built upon identification and consideration of mission objectives and sub-objectives, as appropriate to identify all relevant dimensions of performance. Risk and uncertainty profiles of corresponding performance measures for safety, technical, cost, schedule, and security execution domains developed via comprehensive risk analysis	Apply comprehensive scope and rigor across programmatic, engineering, institutional, partnership, and enterprise domains, addressing mission technical, cost, schedule, safety, and security performance. RIDM built upon identification and consideration of mission objectives and sub-objectives, as appropriate to identify all relevant dimensions of performance. Risk and uncertainty profiles of corresponding performance measures for safety, technical, cost, schedule, and security execution domains developed via comprehensive risk analysis	Apply comprehensive scope and rigor across programmatic, engineering, institutional, partnership, and enterprise domains, addressing mission technical, cost, schedule, safety, and security performance. RIDM built upon identification and consideration of principal mission objectives, as appropriate to identify the critical dimensions of performance. Risk and uncertainty profiles of corresponding performance measures for safety, technical, cost, schedule, and security execution domains developed via comprehensive risk analysis and AoA. Formal	Apply limited scope and rigor across programmatic, engineering, institutional, partnership, and enterprise domains, focused on critical areas where failure would result in injru to personnel or collateral damage. RIDM emphasis is on key safety objectives to “Do No Harm” to systems or missions across the payload interfaces. Safety risk profiles developed via qualitative risk analysis and AoA. Informal deliberation criteria and process defined, applied, and documented to support key decisions.

SMA Area	CLASS A	CLASS B	CLASS C	CLASS D
	and AoA. Formal deliberation criteria and process defined, applied, and documented to support key decisions.	and AoA. Formal deliberation criteria and process defined, applied, and documented to support key decisions.	deliberation criteria and process defined, applied, and documented to support key decisions.	

Appendix E. Assurance Implementation Matrix

E.1 This Assurance Implementation Matrix is used by projects to document their planned implementation consistent with the mission or instrument risk classification(s) and SMA objectives in Appendix D.

E.2 Mission Directorates may choose to invoke a MAR document on a program or project that serves as the baseline set of mission assurance requirements. If the OSMA has concurred with the Mission Directorate's determination to invoke their MAR on a program or project, programs or projects achieve compliance with the invoked Mission Directorate MAR (e.g., SMD Standard Mission Assurance Requirements Payload Classification: D) in lieu of establishing a Assurance Implementation. Matrix.

E.3 Instructions for completing each column of the Assurance Implementation Matrix are as follows:

a. NPR 8705.4 Risk Tolerance Class Objectives and Approved Standards: Include the objectives and accepted standards provided in Appendix D corresponding with the risk tolerance class designated to associated mission or instrument.

b. Objective Satisfied (Y/N): Provide a "Yes" or "No" answer to whether the project plans to satisfy the corresponding objective provided.

c. Project Implementation: Document the project-specific implementation to satisfy the corresponding objective provided , including any approaches provided in the associated NASA-accepted standard(s).

d. Alternate Approaches and Standards: Include details for any alternate approaches or standards proposed and the related project-specific implementation to satisfy the corresponding objective provided.

Topic in Appendix D of NPR 8705.4	NPR 8705.4 Risk Tolerance Class Objectives and Approved Standards	Objective Satisfied (Y/N)	Project Implementation	Alternate Approaches and Standards
Fault Tolerance (including SPFs), Reliability, and Maintainability				
Environmental Test Program Verification and Validation				
Electronics, Electrical, and Electromechanical (EEE) Parts				

Materials				
Telemetry Coverage for Critical Events				
Quality Assurance and Quality Engineering				
Software				
Risk Informed Decision Making (RIDM) and Continuous Risk Management (CRM) Processes				

Appendix F. References

F.1 NPD 1000.3, The NASA Organization.

F.2 NPD 8730.5, NASA Quality Assurance Program Policy.

F.3 NPR 7120.8, NASA Research and Technology Program and Project Management Requirements.

F.4 NPR 7123.1, NASA Systems Engineering Processes and Requirements.

F.5 NPR 7150.2, NASA Software Engineering Requirements.

F.6 NPR 8000.4, Agency Risk Management Procedural Requirements.

F.7 NPR 8020.12, Planetary Protection Provisions for Robotic Extraterrestrial Missions.

F.8 NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.

F.9 NPR 8705.6, Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments.

F.10 NPR 8715.3, NASA General Safety Program Requirements.

F.11 NPR 8715.5, Range Flight Safety Program.

F.12 NPR 8715.6, NASA Procedural Requirements for Limiting Orbital Debris and Evaluating the Meteoroid and Orbital Debris Environments.

F.13 NPR 8715.7, Expendable Launch Vehicle (ELV) Payload Safety Program.

F.14 NPR 8735.1, Exchange of Problem Data Using NASA Advisories and the Government-Industry Data Exchange Program (GIDEP).

F.15 NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects.

F.16 NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft.

F.17 NASA-STD-8729.1, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems.

F.18 NASA-STD-8739.8, Software Assurance Standard.

F.19 NASA-STD-8739.10, Electrical, Electronic, and Electromechanical (EEE) Parts Assurance Standard.