NASA Procedural Requirements

NPR 8705.4
Effective Date: June 14, 2004
Expiration Date: June 14, 2018

COMPLIANCE IS MANDATORY

Risk Classification for NASA Payloads (Revalidated w/change 2 dated June 12, 2013)

Responsible Office: Office of Safety and Mission Assurance

TABLE OF CONTENTS

Appendix B. Classification Considerations for NASA Class A-D Payloads

Appendix C. Recommended SMA-Related Program Requirements for NASA Class A-D Payloads

Change History

NPR 8705.4, Risk Classification for NASA Payloads

Chg #	Date	Description/Comments
1	07/09/08	Admin changes to correct title changes and other admin changes
2	6/12/13	Administrative changes to bring the NPR in compliance with NPR 1400.1 and to improve clarity and avoid duplication.

Preface

P.1 PURPOSE

This NPR establishes baseline criteria that enable a user to define the risk classification level for NASA payloads on human- or nonhuman-rated launch systems or carrier vehicles and the design and test philosophy and the common assurance practices applicable to each level. The establishment of the risk level early in programs and projects provides the basis for program and project managers to develop and implement appropriate mission assurance and risk management strategies and requirements and to effectively communicate the acceptable level of risk.

P.2 APPLICABILITY

a. This NPR applies to NASA Headquarters, NASA Centers, including Component Faciities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory and other contractors only to the extent specified or referenced in their appropriate contracts.

b This document applies to programs and projects governed by NPR 7120.5, NASA Space Flight Program and Project Management Requirements.

c. This NPR applies to NASA payloads and does not apply to launch systems or carrier vehicles. Application of this NPR to on-orbit services or non-NASA payloads provided to NASA as a result of foreign collaborations is at the discretion of the responsible NASA Mission Directorate.

d. This NPR takes precedence over all other lower level documents.

e. The following definitions apply:

(1) Payload - Any airborne or space equipment or material that is not an integral part of the carrier vehicle (i.e., not part of the carrier aircraft, balloon, sounding rocket, expendable or recoverable launch vehicle). Included are items such as free-flying automated spacecraft, Space Shuttle payloads, Space Station payloads, Expendable Launch Vehicle payloads, flight hardware and instruments designed to conduct experiments, and payload support equipment.

(2) NASA Payload - Any payload for which NASA has design, development, test, or operations responsibility.

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

P.3 AUTHORITY

NPD 8700.1, NASA Policy for Safety and Mission Success.

P.4 APPLICABLE DOCUMENTS AND FORMS

a. NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy.

b. NPD 8730.5, NASA Quality Assurance Program Policy.

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

d. NPR 8000.4, Agency Risk Management Procedural Requirements.

e. NPR 8705.5, Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Sucess.

f. NPR 8735.1, Procedures For Exchanging Parts, Materials, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program and NASA Advisories.

g. NPR 8735.2, Management of Government Quality Assurance Functions for NASA Contracts.

P.5 MEASUREMENT/VERIFICATION

Compliance by programs and projects with the requirements contained within this NPR is verified as part of selected life cycle reviews, and by assessments, reviews, and audits. This NPR specifies development of milestone products and control plans that are reviewed at each of the selected life cycle reviews conducted in accordance with the requirements of NPR 7120.5, NASA Space Flight Program and Project Management Requirements, and NPR 7123.1, NASA Systems Engineering Processes and Requirements. Compliance with the requirements contained within this NPR is also monitored by Centers, Mission Directorates, and by the SMA Technical Authority.

P.6 CANCELLATION

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

REVALIDATED W/CHANGE 2, JUNE 6, 2013, ORIGINAL SIGNED BY:

/S/ Bryan O'Connor
Associate Administrator for
Safety and Mission Assurance

DISTRIBUTION:

NODIS

CHAPTER 1. General Information

1.1 Overview

1.1.1 NPR 7120.5, NASA Space Flight Program and Project Management Requirements, defines acceptable risk as the risk that is understood and agreed to by the program project, Governing Program Management Council (GPMC), Mission Directorate, and other customer(s) such that no further specific mitigating action is required. (Some mitigating actions might have already occurred.).

1.1.2 All parties are better able to understand the acceptable risk associated with a program or project when authorization documents and Level 1 requirements include information regarding the relative risk level.

1.1.3 The basic assurance principles and practices associated with the different risk classification levels as indicated in Appendix B are included to further strengthen the understanding and communication at all levels of the NASA organization and program and project teams.

1.2. Risk Classification Development

1.2.1 As early in the formulation process as possible, the Mission Directorate establishes the acceptable risk classification level for each NASA and NASA-sponsored payload. As with all requirements, the risk classification level may evolve throughout the iterative formulation process, but shall be formally documented and approved in program and project plans and Level 1 requirements prior to the Preliminary Design Review and transition into the implementation phase.

1.2.2 For consistency in definition, four risk levels or classifications have been characterized in Appendix B. The classification levels define a hierarchy of risk combinations for NASA payloads by considering such factors as criticality to the Agency Strategic Plan, national significance, availability of alternative research opportunities, success criteria, magnitude of investment, and other relevant factors.

1.2.3 Any equipment that constitutes a payload, or part of a payload, may be separately classified. For example, a Class A satellite may incorporate multiple instruments individually classified A through D.

1.3. Assurance Program Development and Implementation

1.3.1 With the acceptable risk classification level established, using Appendix C as the guideline, the project can define and apply the appropriate design and management controls, systems engineering processes, mission assurance requirements, and risk management processes. Guidelines for safety, mission assurance, design, and test are provided in Appendix C.

1.3.2 Centers and Mission Directorate may develop and update policies, standards, and guidelines to adapt and expand upon the examples in Appendix C for the unique needs of their programs and projects. Each subset of guidelines described by the examples in Appendix C is intended to serve as a starting point for establishment of assurance criteria, mission design, and test programs tailored to the needs of a specific project. The intent is to generate discussion of implementation methodologies

in order for the programs, projects, Centers, the GPMC, and the Mission Directorate to make informed decisions.

1.3.3 This does not limit or constrain the flexibility of a project to deviate from the guidelines, provided that the concurrence and approvals of cognizant Center organizations, GPMCs, and the Mission Directorate are obtained for the specific project approach.

1.3.4 Regardless of risk classification level designation, all payloads should be developed using sound management, engineering, manufacturing, and verification practices.

1.3.5 The Chief, Safety and Mission Assurance exercises general oversight and coordinates Agencywide implementation of this NPR.

CHAPTER 2. Risk Classification Requirements

2.1 Mission Directorate shall:

a. Establish and document the risk classification level for each payload or payload element (Requirement 32917). The Mission Directorate may establish the class designation at the level of assembly it considers appropriate for each project.

b. Establish a set of mission Level 1 requirements for each payload or payload element that reflects the key objectives of the program (Requirement).

c. Notify the NASA Chief Engineer and the Chief, Safety and Mission Assurance of the assigned payload risk classification level (Requirement).

2.2 Project offices shall:

a. Recommend to the Mission Directorate and GPMC a risk classification level designation for proposed payload or payload element (Requirement).

b. Recommend to the Mission Directorate and GPMC appropriate risk classification levels for lower levels of assembly (Requirement).

c. Document the implementation of a balanced acquisition and development approach for achieving the risk classification level designated, and provide it to the Mission Directorate and GPMC (Requirement).

d. Obtain concurrence from cognizant Center organizations, GPMC, and the Mission Directorate for deviations from the project approach for achieving the risk classification designated (Requirement).

e. Maintain project approval documentation to include current risk classification level designation and any changes to the initial risk classification level, together with a description of any deviations from the guidelines in Appendix C (Requirement). This is typically documented in the risk management section of the project plan.

2.3 The Chief, Safety and Mission Assurance shall support Mission Directorates in the development and review of payload risk classification level designations. (Requirement).

2.4 Center Safety and Mission Assurance organizations shall provide input to the project office assessment and recommendation of risk classification levels and assess the risks associated with the tailoring selections of Center safety and mission assurance requirements per Appendix C (Requirement).

2.5 The Office of the Chief Engineer shall serve as the Agencywide focal point for collection and correlation of payload risk classification levels and in-flight failure information and dissemination of lessons learned. (Requirement).

Appendix A - Acronyms

COTS	Commercial-Off-the-Shelf
ESSP	Earth Systems Science Pathfinder
FMEA/CIL	Failure Modes and Effects Analysis/Critical Items List
GAS	Get Away Special
GIDEP	Government Industry Data Exchange Program
GOES	Geostationary Operational Environmental Satellite
IPAO	Independent Program Assessment Office
ISS	International Space Station
IV&V	Independent Verification and Validation
JIMO	Jupiter Icy Moons Orbiter
MER	Mars Exploration Rover
MIDEX	Medium Class Explorers
MRO	Mars Reconnaissance Orbiter
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NPSL	NASA Parts Selection List INPSL): http://nepp.nasa.gov/npsl
GPMC	Governing Program Management Council
PRA	Probabilistic Risk Assessment
SCD	Source Control Drawing
SMA	Safety and Mission Assurance
SMEX	Small Explorer
SPF	Single Point Failure

Appendix B - Classification Considerations for NASA Class A-D Payloads

Four risk levels or classifications have been characterized in Appendix A. The classification considerations in this appendix provide a structured approach for defining a hierarchy of risk combinations for NASA payloads by considering such factors as criticality to the Agency Strategic Plan, national significance, availability of alternative research opportunities or reflight opportunities, success criteria, magnitude of investment, and other relevant factors. Additional or alternate classification considerations may be applied to a specific payload or payload element. The importance weighting assigned to each consideration is at the discretion of the responsible Mission Directorate.

Characterization	Class A	Class B	Class C	Class D
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National significance	Very high	High	Medium	Low to medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission	Long, >5years	Medium, 2-5 years	Short,	Short < 2 years
Cost	High	High to medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to none
In-Flight Maintenance	N/A	Not feasible or difficult	Maybe feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities

Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.
Examples	HST, Cassini, JIMO, JWST	MER, MRO, Discovery payloads, ISS Facility Class Payloads, Attached ISS payloads	ESSP, Explorer Payloads, MIDEX, ISS complex subrack payloads	SPARTAN, GAS Can, technology demonstrators, simple ISS, express middeck and subrack payloads, SMEX

NOTES:

1. Mission impact; i.e., loss of function effect on other payloads or ISS operations may also be a characterization factor. For example, loss of the function of freezers and centrifuges may impact other payloads and increase the overall level of risk.

2. The safety risk to crew inherent in the operation of a human-crewed vehicle may be a factor in payload classification determinations. Class C and D payloads that have a medium or high risk of not achieving mission success may be considered unsuitable for launch on a crewed vehicle, unless they are secondary payloads making use of available launch capacity that would otherwise go unused.

3. Other situation-dependent payload classification considerations may include human-rating environment, logistics support, and interoperability interfaces.

Appendix C - Recommended SMA-Related Program Requirements for NASA Class A-D Payloads

	CLASS A	CLASS B	CLASS C	CLASS D
Single Point Failures (SPFs)	Critical SPFs (for Level 1 requirements) are not permitted unless authorized by formal waiver. Waiver approval of critical SPFs requires justification based on risk analysis and implementation of measures to mitigate risk.	Critical SPFs (for Level 1 requirements) may be permitted but are minimized and mitigated by use of high reliability parts and additional testing. Essential spacecraft functions and key instruments are typically fully redundant. Other hardware has partial redundancy and/or provisions for graceful degradation.	Critical SPFs (for Level 1 requirements) may be permitted but are mitigated by use of high reliability parts, additional testing, or by other means. Single string and selectively redundant design approaches may be used.	Same as Class C.
Engineering Model, Prototype, Flight, and Spare Hardware	Engineering model hardware for new or modified designs. Separate prototype and flight model hardware. Full set of assembled and tested "flight spare" replacement units.	Engineering model hardware for new or significantly modified designs. Protoflight hardware (in lieu of separate prototype and flight models) except where extensive qualification testing is anticipated. Spare (or refurbishable prototype) hardware as needed to avoid major program impact.	Engineering model hardware for new designs. Protoflight hardware permitted (in lieu of separate prototype and flight models). Limited flight spare hardware (for long lead flight units).	Limited engineering model and flight spare hardware.
Qualification, Acceptance, and Protoflight Test Program	Full formal qualification and acceptance test programs and integrated end-to-end testing at all hardware and software levels.	Formal qualification and acceptance test programs and integrated end-to-end testing at all hardware levels. May use a combination of qualification and protoflight hardware. Qualified software simulators used to verify software and system.	Limited qualification testing for new aspects of the design plus full acceptance test program. Testing required for verification of safety compliance and interface compatibility.	Testing required only for verification of safety compliance and interface compatibility. Acceptance test program for critical performance parameters.
EEE Parts *http: // nepp .nasa .gov/ npsl	NASA Parts Selection List (NPSL)* Level 1, Level 1 equivalent Source Control Drawings (SCDs), and/or requirements per Center Parts Management Plan.	Class A requirements or NPSL Level 2, Level 2 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B or NPSL Level 3, Level 3 equivalent SCDs, and/or requirements per	Class A, Class B, or Class C requirements, and/or requirements

			Center Parts Management Plan.	per Center Parts Management Plan.
Reviews	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and code.	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and peer reviews of code.	Full formal review program. Independent reviews managed at Center level with Mission Directorate participation. Include formal inspections of software requirements, peer reviews of design and code.	Center level reviews with participation of all applicable directorates. May be delegated to Projects. Peer reviews of software requirements and code.
Safety	Per all applicable NASA safety directives and standards.	Same as Class A.	Same as Class A.	Same as Class A.
Materials	Verify heritage of previously used materials and qualify all new or changed materials and applications/configurations. Use source controls on procured materials and acceptance test each lot/batch.	Use previously tested/flown materials or qualify new materials and applications/configurations. Acceptance test each lot of procured materials.	Use previously tested/flown materials or characterize new materials. Acceptance test sample lots of procured materials.	Requirements are based on applicable safety standards. Materials should be assessed for application and life limits.
Reliability NPD 8720.1	Failure mode and effects analysis/critical items list (FMEA/CIL), worst-case performance, and parts electrical stress analysis for all parts and circuits. Mechanical reliability, human, and other reliability analysis where appropriate.	FMEA/CIL at black box (or circuit block diagram) level as a minimum. Worst-case performance and parts electrical stress analysis for all parts and circuits.	FMEA/CIL scope determined at the project level. Analysis of interfaces. Parts electrical stress analysis for all parts and circuits.	Analysis requirements based on applicable safety requirements. Analysis of interface.
Fault Tree Analysis	System level qualitative fault tree analysis.	Same as Class A.	Same as Class A.	Fault tree analysis required for safety critical functions.
Probabilistic Risk Assessment NPR 8705.5	Full Scope, addressing all applicable end states per NPR 8705.5.	Limited Scope, focusing on mission-related end-states of specific decision making interest per NPR 8705.5.	Simplified, identifying major mission risk contributors.Other discretionary applications.	Safety only.Other discretionary applications.

Maintainability[1] NPD 8720.1	As required by NPD 8720.1	Application of NPD 8720.1 determined by program. (Typically ground elements only.)	Maintainability considered during design if applicable.	Requirements based on applicable safety standards.
Quality Assurance NPD 8730.5 NPR 8735.2 (NPR 8735.1)	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, and stringent surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, moderate surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, tailored surveillance. GIDEP failure experience data and NASA Advisory process.	Closed-loop problem reporting and corrective action, configuration management, GIDEP failure experience data and NASA Advisory process. Other requirements based on applicable safety standards.
Software	Formal project software assurance program. Independent Verification and Validation (IV&V) as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance insight. IV&V as determined by AA OSMA.
Risk Management NPR 8000.4	Risk Management Program. Risk reporting to GPMC.	Same as Class A.	Same as Class A.	Same as Class A.
Telemetry Coverage[2]	During all mission critical events to assure data is available for critical anomaly investigations to prevent future recurrence.	Same as Class A.	Same as Class A.	Same as Class A.

NOTES:

[1]For ISS payloads, maintainability, reliability, and availability requirements should be defined at an early phase and plans addressed during the design, development, and testing of the payload, regardless of class. Components with low reliability should be assessed for on-orbit maintainability based on the availability requirements, and other relevant factors. The balance of these factors should result in a payload that meets performance requirements for the required duration of flight.

[2]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. 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.