

| [NODIS Library](#) | [Program Management\(8000s\)](#) | [Search](#) |



NASA Procedural Requirements

NPR 8705.5A
Effective Date: June 07, 2010
Expiration Date: June 07, 2015

COMPLIANCE IS MANDATORY

Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects

Responsible Office: Office of Safety and Mission Assurance

Table of Contents

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents
- P.5 Measurement/Verification
- P.6 Cancellation

Chapter 1. Introduction

- 1.1 Background
- 1.2 PRA Characteristics

Chapter 2. PRA Process

- 2.1 Overview
- 2.2 Definition of PRA Objective(s)
- 2.3 PRA Requirements
- 2.4 Scenario Development
- 2.5 Quantification and Uncertainty
- 2.6 Interpretation of the PRA Result
- 2.7 PRA Documentation
- 2.8 PRA Quality

Chapter 3. PRA Scope and Level of Detail

- 3.1 Overview

3.2 Program Life-Cycle Phases

3.3 Application of PRA to Support Decisions

Chapter 4. Roles and Responsibilities

4.1 Overview

4.2 Mission Directorate Associate Administrators

4.3 Chief, Safety and Mission Assurance

4.4 Center Directors

4.5 Center Safety and Mission Assurance (SMA) Directors

4.6 Program/Project Managers

4.7 Program/Project PRA Lead

Chapter 5. Independent Peer Reviews (IPR)

5.1 Overview

5.2 IPR Authority

Appendix A. Acronyms

Appendix B. References

Appendix C. Comments on PRA Scope

Preface

P.1 Purpose

This NASA Procedural Requirements (NPR) provides basic requirements for performing a probabilistic risk assessment (PRA) for NASA programs and projects. It addresses technical, mission success, safety, and health risk. It does not address programmatic risk involving consideration of cost and schedule.

P.2 Applicability

- a. This NPR 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, other contractors, grant recipients, or parties to agreements to the extent specified or referenced in the appropriate contracts, grants, or agreements.
- b. This NPR applies specifically to programs and projects that provide aerospace products or capabilities; i.e., space and aeronautics systems and launch, flight, and control systems that support the mission. The importance and scope (potential effects on public and worker health and safety, strategic significance, and cost) of the project/program being assessed is used to identify the extent of the PRA application.
- c. This NPR does not apply to other types of programs and projects such as research and technology development and related test facilities, ground test infrastructure, training, or education; however, the PRA concepts and practices described within this document can be beneficial to other projects.
- d. The applicability of this NPR to programs/projects already in progress depends on its criticality and life-cycle phase. Decisions concerning applicability to programs/projects in progress will be made on a case-by-case basis involving program/project manager recommendations to the governing program management council (PMC).

P.3 Authority

- a. NPD 1000.5, Policy for NASA Acquisition.
- b. NPD 7120.4, Program/Project Management.
- c. NPD 8700.1, NASA Policy for Safety and Mission Success.
- d. NPR 7120.5, NASA Space Flight Program and Project Management Requirements.
- e. NPR 8000.4, Agency Risk Management Procedural Requirements.
- f. NPR 8715.3, NASA General Safety Program Requirements.

P.4 Applicable Documents

- a. Code of Federal Regulations, Title 22 Foreign Relations, Part 120-124 International Traffic In Arms Regulations.

- b. NPD 1440.6, NASA Records Management.
- c. NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy.
- d. NPR 1441.1, NASA Records Retention Schedules.
- e. NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments.

P.5 Measurement/Verification

The Office of Safety and Mission Assurance (OSMA) verifies program/project compliance with the requirements in the NPR through audits performed in accordance with NPR 8705.6, Safety and Mission Assurance Audits, Reviews, and Assessments, and through peer review. The program/project documents compliance with the requirements in this NPR in their program/project planning documentation and their PRA report.

P.6 Cancellation

NPR 8705.5 dated July 12, 2004.

/S/

Bryan O'Connor
Chief, Safety and Mission Assurance

Chapter 1. Introduction

1.1 Background

1.1.1 A PRA is a structured, logical analysis methodology that is used for identifying and assessing risks in a variety of applications including complex technological systems. In general, a PRA provides a modeling framework that interfaces with or includes the various disciplines used to conduct health, safety, and mission assurance analyses including hazard analysis, failure mode and effects analysis, and reliability analysis. A PRA draws upon the relevant collection of qualitative and quantitative information and models that are developed as part of design and assurance activities.

1.1.2 A PRA is applicable to all program/project life-cycle phases: formulation (Pre-Phase A - Phase B), implementation (Phase C - Phase E), and closeout (Phase F). The scope, level of detail and type of information that are necessary, and the types of scenarios modeled may vary during the assessment of each life-cycle phase and its intended application. A PRA will have varying degrees of complexity and fidelity depending on the program/project life-cycle phase and the decisions being supported. High-level PRAs performed during formulation and early design may be used to compare and establish meaningful safety, health, and performance requirements for mission and architectural concepts. Later in the design, more focused PRAs may be performed to compare risks associated with proposed design solutions. As the program/project nears implementation, the PRA grows in complexity and fidelity to provide an integrated model of an entire mission or facility, including its architectural, mechanical, human, and software components.

1.1.3 NPD 1000.5, Policy for NASA Acquisition, requires the incorporation of a risk-informed acquisition process that includes the assessment of technical, safety, and health risks among others. In addition, for each life-cycle phase and application, PRA facilitates Agency risk management activities required by NPD 7120.4, Program/Project Management, and NPR 8000.4, Agency Risk Management Procedural Requirements. Risk analyses of decision alternatives that include the quantification and comparison of safety, health, and technical performance measures are used in the risk-informed decision making (RIDM) process. When decision alternatives are selected to define a program or project, a PRA is conducted to characterize weaknesses and vulnerabilities in design and implementation that can adversely impact safety and health, performance, and mission success. Those events that contribute most to risk and uncertainty can be identified by the PRA and provide the focus for further assessment and risk management strategies. These risk management activities can reveal where alternatives, changes in design and operation, and/or cost-effective expenditure of resources can be made to improve design and operation and inform the decision-makers of uncertainties that may need to be addressed.

1.1.4 The Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners is a companion document to this NPR and provides further details on PRA methodology for aerospace applications. Many references are made to this companion document for practical advice on performing PRAs.

1.2 PRA Characteristics

1.2.1 PRA is applied to identify and evaluate risks affecting safety and health; i.e., having a potential for injury or illness, loss of life, damage, or unexpected loss of equipment, as well as those affecting the ability to reliably meet mission objectives (e.g., due to equipment failure).

1.2.2 A PRA characterizes risk in terms of three basic questions: (1) What can go wrong? (2) How likely is it? and (3) What are the consequences? The PRA process answers these questions by systematically identifying, modeling, and quantifying scenarios that can lead to undesired consequences, considering uncertainties in the progression of such scenarios due to both variations of, and limited knowledge about, the system and its environment. The PRA integrates models based on systems engineering, probability and statistical theory, reliability and maintainability engineering, physical and biological sciences, decision theory, and expert elicitation. The collection of risk scenarios allows the dominant contributors to risk and areas of uncertainty about risk to be identified.

1.2.3 PRA generally consist of complex chains of events (or scenarios), each of which can lead to an undesired consequence or end state. Examples of such events include failures of hardware and software system elements, human actions or lack thereof, and phenomenological events such as degradation or debris impacts. Complex scenarios may include events whose implications separately appear to be slight or insignificant but collectively can combine and interact to cause high severity consequences. The total probability from the set of scenarios modeled may also be non-negligible even though the probability of each scenario is small.

1.2.4 The assessment normally takes place in the context of safety, health, and mission success criteria that specify a minimum required level of confidence that loss of life and equipment will be avoided, and mission objectives will be achieved. While elements of such requirements may be allocated to other disciplines; e.g., hardware reliability, the PRA provides an integral modeling framework in which various elements can be represented.

1.2.5 A PRA is conducted using a systematic process to assess operational objectives, application(s), and scope; model scenarios that can lead to undesired consequences or end states; quantify scenario probabilities and consequences, as applicable, including the characterization of uncertainty; and provide and interpret results for the decision(s) being supported. Documentation and communication are also important parts of the PRA process.

1.2.6 Two examples of PRAs are provided in the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.

Chapter 2. PRA Process

2.1 Overview

2.1.1 The process for conducting a PRA is shown in Figure 1. This process starts with the definition of objectives and ends with the documentation of the results. Deviations from the process and techniques summarized below may be necessary based on the objectives and scope of the PRA. These deviations need to be approved before implementation.

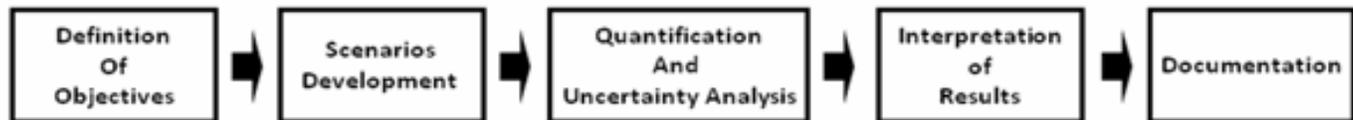


Figure 1. PRA Process

2.2 Definition of PRA Objective(s)

2.2.1 The program/project manager shall:

a. Ensure that a PRA is conducted for: (i) payloads with a risk classification level of A, as defined in NPR 8705.4 ([Requirement 69148](#));(ii) Category I programs/projects as defined in NPR 7120.5([Requirement 69149](#));(iii) any other program or project determined by the program manager to meet the criteria of Priority Ranking I programs/projects as defined in NPR 8715.3 ([Requirement 69150](#)).

b. Determine whether a PRA is necessary for: (i) Priority Ranking II programs/projects as identified in Chapter 2 of NPR 8715.3, NASA General Safety Program Requirements ([Requirement 69152](#))

; and (ii) payloads with a risk classification level of B, as defined in NPR 8705.4, Risk Classification for NASA Payloads ([Requirement 69153](#)).

c. Request concurrence from the SMA Technical Authority if the determination is made (see paragraph 2.2.1.b) that a PRA is not necessary for (i) Priority Ranking II programs/projects as identified in Chapter 2 of NPR 8715.3, NASA General Safety Program Requirements([Requirement 69155](#))

; and (ii) payloads with a risk classification level of B, as defined in NPR 8705.4, Risk Classification for NASA Payloads ([Requirement 69156](#)).

d. Define the objective(s) of the PRA and its intended applications to support decisions and technical reviews for selected life-cycle phases([Requirement 69157](#)).

Note: The objectives and intended applications provide information needed to define the scope, level of detail, schedule, and end states (performances measures) of the PRA which are based on the program/project life-cycle phase and the decisions being supported prior to and during a specific technical review.

e. Decide the uses (and life-cycle phases) that are supported by a PRA for existing programs/projects ([Requirement 69159](#)).

2.2.2 The PRA lead shall:

a. Describe the scope and level of detail of the PRA, including the identification of end-states (undesirable consequences, performance measures, figures of merit) of interest, which are consistent with the PRA objectives and applications defined in paragraph 2.2.1 of this NPR and documented in the approved PRA plan ([Requirement 33035](#)). (See Chapter 3 of this NPR.)

b. Define quantitative performance measures and numerical criteria that are evaluated by the PRA consistent with the objectives and application defined in the approved PRA plan ([Requirement 69148](#)).

c. Develop a PRA schedule compatible with the objectives, applications, and life-cycle phases identified by the program/project manager ([Requirement 69163](#)).

2.3 PRA Requirements

2.3.1 The type of information required and the types of scenarios modeled will vary during the assessment of each program/project life-cycle phase dependent on the decisions supported and the associated technical reviews and Key Decision Points (KDP) (see NPR 7123.1A, NASA Systems Engineering Process and Requirements). Some deviation from the results summarized below may be necessary as long as the PRA meets program/project safety and health objectives.

2.3.2 The PRA lead shall conduct a systematic and comprehensive PRA applicable to the decisions and program/project life-cycle phase being supported that includes definition of objectives, scenario development, quantification and uncertainty analysis, interpretation of results, and documentation consistent with the approved PRA plan ([Requirement 69166](#)).

2.4 Scenario Development

2.4.1 An accident scenario starts with an initiating event and progresses through a series of successes or failures of intermediate events leading to a defined end state. A PRA attempts to identify and quantify all applicable scenarios. The identification of the scenarios involves a thorough understanding of the decisions being supported and the program/project concepts, architecture, systems, and operations to be modeled including the success states (conditions or parameters for success) needed to fulfill mission objectives; the identification of the initiating events that mark the beginning of the accident scenarios; and an understanding of the failure causes (or their complements, successes) of each event in the accident scenarios.

(See the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners)

2.4.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Define the concept, mission, architecture, system, and/or operation, including the identification and definition of applicable mission success criteria, being assessed to support specific decisions and life-cycle phase(s) ([Requirement 69170](#)).

Note: The information needed to describe the design and operation of the system may consist of Baseline Concept Documents, functional descriptions, operating manuals, drawings, schematics, parts lists, materials, hardware maps, specifications, and interface descriptions. Existing data/products should be utilized whenever possible to avoid duplication of effort and ensure product consistency. If little or no documentation is available to perform scenario and failure modeling, the analyst not familiar with the technology will need to interview engineers and operating crews supporting the design for the project to ensure an understanding of how the system is intended to be or being operated. In this case, the best possible description that can be developed for design and operation based on interview notes can be used for the analysis.

b. Identify and describe the contributing set of initiating events that were used to initiate accident scenarios leading to the defined end states ([Requirement 69172](#)) including:

(1) The initiating events that are not included in the assessment and the rationale for exclusion ([Requirement 69173](#)).

(2) Any initiating events that are treated as a group, their group initiator frequencies, and the techniques used to derive the group initiator frequencies ([Requirement 69174](#)).

Note: See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.

c. Identify and describe the accident scenarios leading to the defined end states including the initiating events, intermediate events, and contributing conditions ([Requirement 69176](#)) including:

Note: The review of applicable Hazard Analyses and Failure Mode and Effects Analyses can be used to identify accident contributors and accident scenarios. In those cases where the Hazard Analysis is not complete or available, the PRA analyst can interview safety engineers, design engineers and operations personnel to identify a list of possible hazards. In those cases where these analyses are not complete or available, the PRA analyst can interview reliability engineers, design engineers and operating crews to identify a list of possible failure modes that may impact safety and health, and mission success.

(1) The models and techniques used to identify the accident scenarios ([Requirement 69178](#)).

(2) The phenomenological variables and the timing or event sequencing modeled ([Requirement 69179](#)).

Note: Phenomenological variables are those parameters used to characterize the scenario being evaluated or modeled, such as knowing the size of the orbital debris hitting the vehicle, the radiation levels, and the strength of materials, fluid pressure, and fluid temperature.

d. Identify and describe the analytical techniques (reliability and failure models) used to assess the accident scenario event probabilities including their failure causes ([Requirement 69181](#)).

2.5 Quantification and Uncertainty

2.5.1 Quantification refers to the process of evaluating the probability (or frequency) and the severity of the consequences associated with the end states. The frequency of occurrence of each end state is the logical product of the initiating event frequency and the (conditional) probabilities of the intermediate event along the scenario path from the initiating event to the end state. Quantification involves the collection and analysis of data and information in order to estimate various parameters of the PRA model, including event probabilities and consequence severities, and the treatment of uncertainty (both aleatory and epistemic) in these parameters and the overall results. Uncertainty analysis captures both the randomness in physical processes and the uncertainty in knowledge of the processes, models, and parameters used in the analysis. (See the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners)

2.5.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Quantify the probability, including uncertainty, for each event in the accident scenario described in paragraphs 2.4 above ([Requirement 69185](#)).

b. Quantify the probability, including uncertainty, for the individual accident scenarios ([Requirement 69185](#)).

c. Quantify the total probability, including uncertainty, for each defined end state (summed from all the accident scenarios leading to the same end-state) ([Requirement 69187](#)).

d. Quantify the severity of the end states (if the magnitude of the end state can be quantified) including the uncertainty in end state severity ([Requirement 69188](#)).

e. Describe the data used in quantifying event probabilities and end state severities ([Requirement 69189](#)).

f. Describe the techniques used to propagate the uncertainty in the scenario probabilities and the end state severities ([Requirement 69190](#)).

g. Quantify the uncertainty (accounting for both aleatory and epistemic uncertainties) for all of the probabilities and severities evaluated in the PRA including the effects of sensitivity

assessments ([Requirement 69191](#)).

Note: Aleatory uncertainty is the natural, unpredictable variation (randomness) in the performance of the system or physical processes being studied. Epistemic uncertainty is due to a lack of knowledge about the processes, models, parameters, and behavior used in the analysis.

h. Seek the expertise needed to reduce the epistemic uncertainty to as low an uncertainty as practical ([Requirement 69193](#)).

i. Provide an ordering and description of the major contributors covering events, accident scenarios, and end states ([Requirement 69194](#)).

Note: Importance measures can be used to identify major contributors to risk. If these measures are used, the results should be described in the risk assessment report.

2.6 Interpretation of the PRA Results

2.6.1 The results of the PRA process are interpreted for application to specific decisions that occur during a program/project life-cycle phase and used to support technical reviews. Some applications may include the identification of mission concepts and architectures with minimum risk while other applications may include the design and/or operation of specific systems and/or mission profiles. Key points in interpreting PRA results include the analysis objectives and scope, limitation and assumptions in the analysis and their impact on the results, data used, uncertainty, and the influence of the models (e.g., common-cause, human reliability, software reliability, phenomenological) on the overall results.

2.6.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Provide an interpretation of the results applicable to the PRA objectives, scope, specific decision(s), and life-cycle phase(s) being supported ([Requirement 69199](#)).

b. Explain the overall degree of uncertainty about the results and provide a discussion of the sources of uncertainty ([Requirement 69200](#)).

c. Describe the applicability, limitations, and strengths of the PRA to support and inform decisions and trades ([Requirement 69201](#)).

Note: The applicability, limitation, and strengths of the PRA to support decisions during an applicable technical review should be described.

2.7 PRA Documentation

2.7.1 PRA documentation includes the PRA results, models, data, and supporting information and is maintained under configuration control. Documentation can be in the

form of a summary report and records of detailed supporting models, data, analyses, and information.

2.7.2 Consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall:

a. Produce and maintain a report of the PRA that supports the decisions associated with the specified program/project life-cycle phase and technical review ([Requirement 69206](#)

including:

- (1) the results given in paragraphs 2.3 through 2.6, above,
- (2) the analysis and modeling assumptions,
- (3) the treatment of explicit dependencies, event correlations, and common cause failure modeling,
- (4) the integration of specialized and off-line analyses,
- (5) model integration,
- (6) the principal results obtained including decisions and trade-offs supported, and
- (7) the principal conclusions.

b. Ensure that the detailed PRA models developed, data used, analyses carried out, computer printouts generated, results obtained, and all relevant supporting information are available ([Requirement 692621](#)

c. Develop a presentation package giving the scope, assumptions, and key results for communication purposes ([Requirement 69262](#)).

2.7.3 The program/project manager shall have the authority to approve of the public release of the summary PRA report and access to the supporting models, data, analyses, and information ([Requirement 69263](#))

2.8 PRA Quality

2.8.1 For all PRAs, consistent with the objectives and application defined in the approved PRA plan, the PRA lead shall ensure that the PRA follows quality assurance principles and practices that are analogous to those in other engineering fields including:

a. Assurance of the accuracy, rigor, fidelity, and completeness of the models, scenarios, and data analyses, so that reported results are applicable to the decisions and technical reviews supported ([Requirement 69266](#))

b. The comparison of quantitative results with heritage data for similar systems, subsystems, or components when available ([Requirement 69267](#))

.

c. Use of accepted and justified methods, analytical techniques, and tools that fit the specific application ([Requirement 69268](#))

.

d. Use of validated software with version control and baseline documentation ([Requirement 69269](#))

.

Note: Validated software has been reviewed and benchmarked for the application for which it is being used with documentation that includes a user manual and code description.

e. Maintenance and updating of models as the PRA effort progresses ([Requirement 69271](#))

.

f. Establishment of strong ties with program/project configuration and requirements management activities and operations personnel to ensure that the PRA being developed reflects the latest or the most suitable design ([Requirement 69272](#))

.

g. The use of terminology in the PRA that is consistent with what is used in the program/project in order to facilitate risk communication ([Requirement 69173](#)).

Note: Use consistent terminology for all significant factors that might cause or affect the outcome of an undesired event. Examples include the names of initiating events, mitigating systems, and components.

Chapter 3. PRA Scope and Level of Detail

3.1 Overview

3.1.1 The purpose of a PRA is to provide risk information for decision making during various phases of a program/project life cycle. Risk information is used as input for decisions involving concept, architecture and mission formulation, functional and hardware design after including humans and software, and mission operations. These types of decisions occur during program/project development studies, preliminary and detail design activities, and mission profile studies to support internal and external technical reviews. Specifically, a PRA is developed as part of these activities to help identify alternatives that pose the least risk within program/project constraints and to provide risk information to support program/project technical reviews.

3.1.2 While all program/project life-cycle phases can be supported by a PRA, the best use of the PRA is to support the life-cycle phase activities leading up to System Definition Review/Mission Definition Review (SDR/MDR), Critical Design Review (CDR), Operational Readiness Review/Flight Readiness Review (ORR/FRR), and mission operations where important conceptual, architectural, design, and operational decisions are being made. The program/project life-cycle phase and technical reviews supported by a PRA are illustrated in Figure 2. The type of decisions made during each life-cycle phase varies dependent on the type of program/project (human space flight, robotic, infrastructure, or other) being conducted.

Program / Project Life-Cycle Phase	Pre-Phase A Concept Studies	Phase A Concept and Technology Development	Phase B Preliminary Design & Technology Completion	Phase C Final Design & Fabrication	Phase D System Assembly, Int. & Test, Launch	Phase E Ops & Sustain	Phase F Closeout
Life-cycle Gates		KDPA	KDPB	KDPC	KDPD	KDPE	KDPF
Human Space Flight Programs / Projects Reviews	MCR	SDR	PDR	CDR	ORR, FRR		DR
Robotic Mission Program / Project Reviews	MCR	MDR	PDR	CDR	ORR, FRR		DR

Footnotes: KDP – Key Decision Point, MCR – Mission Concept Review, SDR – System Definition Review, MDR – Mission Definition Review, PDR – Preliminary Design Review, CDR – Critical Design Review, ORR – Operational Readiness Review, FRR – Flight Readiness Review, DR – Decommissioning Review

Figure 2. Key Decision Points and Technical Reviews Supported by PRA

3.1.3 PRAs are conducted to support design, safety, health, and performance decisions as the program/project progresses through its life-cycle phases. The scope, level of detail, and rigor of the PRA are commensurate with the program/project life-cycle phase activity being assessed along with program/project complexity and the severity of the hazards and potential consequences (e.g., human safety and health, mission success, strategic importance).

Additionally, PRA also supports outside stakeholder requirements such as the safety analyses conducted for space nuclear missions (see NSC/PD-25, Scientific or Technological Experiments

with Large-Scale Adverse Environmental Effects and Launch of Nuclear Systems into Space).

3.2 Program Life-Cycle Phases

3.2.1 During the life-cycle of a program/project, risk assessments and risk information can be used to support specific phase activities and decisions and as input to the following technical reviews and phases: SDR/MDR, CDR, and ORR/FRR, and Phase E, Operations and Sustainment. The types of decisions that occur prior to and during these life-cycle phases involve:

- a. Mission architecture, proposed system architecture and design, definition of functional and performance requirements, and the flow down of functional elements of the mission to ensure that the overall concept is complete and feasible.
- b. Detailed design based on a demonstration that the preliminary design meets all system requirements with acceptable risk. Inputs to these decisions involve the selection of design options, the identification of interfaces, and the description of verification methods.
- c. Completion of flight and ground system development and mission operations, meeting mission performance requirements, and authorizing operations (launch, flight, space, or infrastructure) based on system technical maturity, documentation, test data, and analyses that support verification.

3.2.2 A well designed PRA is structured and developed incrementally to be suited to "grow" through the life-cycle phases involving these activities. Detailed discussions of program/project life-cycle phases and technical reviews are given in NPD 7120.4, Program/Project Management, NPR 7120.5, NASA Space Flight Program and Project Management Requirements, NPR 7123.1, NASA Systems Engineering Process and Requirements, and the NASA Systems Engineering Handbook, NASA/SP-2007-6105.

3.3 Application of PRA to Support Decisions

3.3.1 For each program/project life-cycle phase, the PRA lead, in coordination with the PRA team, reviews the decisions that need to be made. Based on the type of program/project (crewed space flight, robotic, nuclear, infrastructure), the specific objectives, input from the program/project manager, and the program/project maturity, the PRA lead and PRA team define the scope and level of detail of the PRA. The PRA addresses technical, mission success, and safety and health risk. It does not address programmatic risk involving the consideration of cost and schedule.

Note: Comments on the development of the scope and level of detail of the PRA are given in Appendix C. A discussion of cost risk assessment is given in the NASA Cost Estimating Handbook (2008).

3.3.2 The PRA lead shall:

- a. Document the plans (level, scope, and approach) for implementing and conducting the PRA in a program/project risk management plan or other planning documentation (e.g., PRA plan, program plan, reliability and maintainability plan) ([Requirement 69290](#)).
- b. Ensure that the PRA plan is approved by the program/project manager and has concurrence from the Center SMA Director prior to conducting the PRA (see Section 4.6.1.c) ([Requirement 69291](#)).

Chapter 4. Roles and Responsibilities

4.1 Overview

4.1.1 NPD 8700.1, NASA Policy for Safety and Mission Success, states that Mission Directorate Associate Administrators, Center Directors, and program/project managers are responsible for assuring that appropriate Agency safety, health, reliability, maintainability, quality, and risk management policies, plans, techniques, procedures, and standards are implemented. This chapter outlines specific responsibilities with regard to PRA.

4.2 Mission Directorate Associate Administrators

4.2.1 Mission Directorate Associate Administrators shall:

- a. Ensure that applicable programs and projects conduct a PRA in accordance with this NPR ([Requirement 69298](#)).
- b. Ensure that PRA results are available and used for informing Agency risk management applications and program/project technical reviews ([Requirement 69299](#)).
- c. Ensure that adequate resources (funding, personnel, methods, data, and software applications) are made available for PRA ([Requirement 69300](#)).
- d. Ensure that formal PRA awareness and methodology training are provided periodically to managers, practitioners, and contractors ([Requirement 69301](#)).

4.3 Chief, Safety and Mission Assurance

4.3.1 The Chief, Safety and Mission Assurance shall:

- a. Develop and maintain NASA PRA policy, procedures, and guidelines and assure their correct implementation at Headquarters and at the Centers ([Requirement 69304](#)).
- b. Provide corporate and functional leadership, mentoring, technical direction, and consultation on PRA methodology (on how to conduct a PRA), PRA tools, and oversight Agency wide ([Requirement 69305](#)). These responsibilities include:
 - (1) Establishing a mechanism for the exchange of PRA-related information (program/project PRA models, data, reports, and peer review results), methodology, best practices, computer applications, training, and lessons learned across programs/projects, Centers, Government agencies, and international partners ([Requirement 69306](#)).
 - (2) Assuring that PRA is adequately planned and conducted and utilizes a valid technical approach and data to support risk management activities ([Requirement 69307](#)).
 - (3) Assisting the Center SMA Directors in their review and approval of program/project PRA plans, when requested ([Requirement 69308](#)).

4.4 Center Directors

4.4.1 Center Directors shall ensure that their SMA and Engineering organizations acquire, maintain, and utilize the appropriate expertise to conduct a PRA and support Center-based PRA programs/projects ([Requirement 69310](#)).

4.5 Center Safety and Mission Assurance (SMA) Directors

4.5.1 Center SMA Directors shall:

- a. Approve or provide upon request by the program/project manager, a PRA lead with experience and demonstrated technical competence in the conduct and application of PRAs for each Center-hosted program/project PRA ([Requirement 69313](#)).
- b. Concur on Center-hosted program/project PRA plans ([Requirement 69314](#)).
- c. Transmit the program/project PRA plan to OSMA prior to conducting the PRA ([Requirement 69315](#)).

4.6 Program/Project Managers

4.6.1 Program/project managers shall:

- a. Ensure that adequate funding for the scope and application of the PRA documented in the approved PRA plan is properly included in the program/project budget to support an IPR, as required ([Requirement 691318](#)).

Note: Decisions on when to conduct an IPR of the PRA are based on program/project complexity, consequence severity, cost, visibility, potential risk, and the key decisions being supported by the PRA at the various technical reviews (See Chapter 5).

- b. Approve of the PRA plan contained in the program/project risk management plan or other program/project planning documentation developed by the PRA lead (e.g., PRA plan, program plan, reliability and maintainability plan)([Requirement 69319](#)).

; (See Paragraph 3.3.2.)

- c. Inform and obtain approval of the program/project PRA plan from the host Center SMA Director for program/project Level 2 (NASA Center-level program management) requirements and implementation plans ([Requirement 69321](#)).

- d. Ensure the results and documentation of the PRA are in accordance with the requirements described in Chapter 2 of this NPR and satisfy the program/project scope and objectives as documented in the approved PRA plan ([Requirement 69322](#)).

- e. Ensure that program/project implementation procedures reflect and incorporate the use of PRA results (including uncertainty) in accordance with the project scope and objectives documented in the approved PRA plan to:

(1) Support RIDM, including the development of performance measures and requirements and continuous risk management ([Requirement 69324](#)).

(2) Identify recommended controls (preventive and mitigating features, compensatory measures) needed to reduce and manage risks ([Requirement 69325](#)).

(3) Update design, operating, implementation, and maintenance plans biannually to reflect insights from PRA ([Requirement 69326](#)).

f. Reduce program/project risk to an acceptable level if the residual risk, as shown through the use of PRA, is deemed unacceptable as defined by program/project requirements documented in the approved PRA plan ([Requirement 69327](#)).

Note: Residual risk is defined as the risk that remains or is introduced following the implementation of prevention and mitigation measures and controls.

g. Ensure that the PRA has internal reviews in order to enhance its quality and credibility and to assure consistency with the requirements of this NPR and the approved PRA plan ([Requirement 69329](#)).

h. Ensure that all PRA inputs, products, models, analyses, and documentation are made readily available for IPRs consistent with the objectives and applications defined in the approved PRA plan ([Requirement 691330](#)).

i. Consistent with the objectives and applications defined in the approved PRA plan, ensure that contracts for PRAs:

(1) Are supported by reliability and maintainability and system safety analyses ([Requirement 69332](#)).

(2) Are properly represented in procurement documents (e.g., requests for proposals, proposals, review criteria, statements of work, procurement plans) to be consistent with program/project level PRA models ([Requirement 69333](#)).

(3) Have PRA requirements from this NPR flowed down including the availability of functional, safety and health, reliability, and risk models, analyses, and relevant data ([Requirement 69334](#)).

(4) Include a schedule with interface deliverables commensurate with the requirements of Paragraph 4.6.1.e and 4.6.1.f ([Requirement 69335](#)).

4.7 Program/Project PRA Lead

4.7.1 Program/project PRA leads shall:

a. Establish a qualified multidisciplinary PRA team to conduct the PRA ([Requirement 69338](#)) in accordance with this NPR and the approved PRA plan, including:

(1) The selection of qualified individuals, with appropriate PRA training, experience, and expertise, that are knowledgeable about the program/project being assessed and the PRA requirements discussed in Chapters 2 and 3 of this NPR.

(2) Representatives from key program/project functional elements (e.g., design, engineering, operation including crew operation, system safety, and maintenance).

(3) Participation, input, and review from appropriate NASA organizations.

b. Ensure that PRA models, results, data, and supporting documentation are baselined for each

technical review and are under configuration control, consistent with the scope and objectives of the approved PRA plan ([Requirement 69342](#)).

Note: The maintenance and safeguarding of records resulting from PRAs is conducted in accordance with NPR 1441.1, NASA Records Retention Schedule.

- c. Provide PRA results and documentation to support and inform internal and external technical reviews in accordance with the project scope and objectives documented in the approved PRA plan ([Requirement 69344](#)).
- d. For PRAs that provide input to other PRAs either at a higher level or for other program/project elements, ensure that the PRA assumptions, models, quantification, and terminology are documented and consistent with the PRAs supported ([Requirement 69345](#)).
- e. Ensure that the PRA is consistent with and supported by system safety analyses and reliability, availability, and maintainability analyses ([Requirement 69346](#)).

4.8 SMA Technical Authority

- a. The SMA Technical Authority shall have the authority to concur or nonconcur in the determination by the program manager that a PRA is not necessary for: (i) Priority Ranking II programs/projects as identified in Chapter 2 of NPR 8715.3, NASA General Safety Program Requirements; and (ii) payloads with a risk classification level of B, as defined in NPR 8705.4, Risk Classification for NASA Payloads ([Requirement 69348](#)).

Chapter 5. IPR

5.1 Overview

5.1.1 An IPR is conducted to assure that the PRA represents the correct risk profile of the system being modeled and supports the decisions being made as documented in the approved PRA plan. These reviews are important for PRAs involving public and employee health and safety, nuclear space missions, and for program/project PRAs involving high cost and strategic importance (Priority Ranking I programs/projects).

5.2 IPR Authority

5.2.1 The SMA Technical Authority shall:

- a. Ensure the organization, coordination, and conduct of an IPR for each PRA of a Priority Ranking I and payload risk classification A program and project (see Chapter 3)([Requirement 69354](#)).
- b. Ensure the coordination of the IPRs with the program/project manager to ensure it is documented in the PRA plan ([Requirement 69355](#)).
- c. Ensure that the IPR is carried out by a team of independent peers including both recognized PRA experts as well as relevant domain experts in the design and mission of the program/project, who are not involved in the study and have no stake in its results ([Requirement 69356](#)).
- d. Ensure the IPR concentrates on the appropriateness of methods, information sources, judgments, and assumptions with respect to the program/project/system application being evaluated and its objective(s) ([Requirement 69357](#)).

Appendix A. Acronyms

CDR	Critical Design Review
FRR	Flight Readiness Review
IPR	Independent Peer Review
KDP	Key Decision Point
MDR	Mission Definition Review
NPR	NASA Procedural Requirements
NPD	NASA Policy Directive
ORR	Operational Readiness Review
OSMA	Office of Safety and Mission Assurance
PD/NSC-25	Presidential Directive/National Security Council Memorandum # 25
PMC	Program Management Council
PRA	Probabilistic Risk Assessment
RIDM	Risk-Informed Decision Making
R&M	Reliability and Maintainability
SDR	System Definition Review
SMA	Safety and Mission Assurance

Appendix B. References

B.1 NPD 1000.3, The NASA Organization.

B.2 NPR 7123.1, NASA Systems Engineering Processes and Requirements.

B.3 NPR 8705.4, Risk Classification for NASA Payloads (Revalidated July 9, 2008).

B.4 Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, August 2002, <http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf>.

B.5 Presidential Directive/National Security Council Memorandum Number 25 (PD/NSC-25), Scientific or Technological Experiments with Possible Large-Scale Adverse Environmental Effects and the Launch of Nuclear Systems into Space.

B.6 NASA Cost Estimating Handbook (2008) (http://ceh.nasa.gov/ceh_2008/2008.htm).

B.7 NASA/SP-2007-6105, NASA Systems Engineering Handbook.

Appendix C. Comments on PRA Scope

C.1 PRA is used to evaluate the risk associated with various alternatives, reference mission concepts, and feasibility studies. Prior to SDR/MDR, the program hardware and mission are in concept development, and the PRA to support program/project implementation may consist of simplified models and be used to gain top level risk insights on the various alternatives.

C.2 When a specific mission concept and architecture are selected and the system requirements defined, the values of the end states or performance metrics determined by the risk assessment provide input to establishing the safety, health, and technical performance requirements for the mission.

C.3 Design generally involves the development of technologically feasible configurations that meet functionality and performance requirements and seek options that best satisfy constraints while minimizing costs and risk to acceptable levels. The PRA that supports the activities leading to CDR may initially consist of high-level and simplified models but with more detail and fidelity for conducting design trade-offs eventually leading to a final design. As the design progresses, the PRA is also refined where more detailed studies are conducted. When the design is ready for fabrication, the PRA is updated to reflect the as-built configuration. From a design standpoint, the maturity, architecture, systems, and assemblies are included in the PRA model for all end states specified in the program/project objectives. The results of this PRA can be compared to established performance requirements and expected operations and to identify margins. The results can also be used to identify critical components (dominant contributors) that may require special attention during fabrication and assembly. Completeness of scenarios is an important consideration of a PRA that supports this life-cycle phase. Uncertainty analysis is performed to provide the decision-maker with a full appreciation of the overall degree of uncertainty about the PRA results and an understanding of which sources of uncertainty are critical to the results that guide decisions.

C.4 The PRA that supports activities leading to ORR/FRR needs to be complete and full scope and reflect the as-built end product. This PRA is used to conduct operations studies and mission profile analyses. A PRA performed prior to operation can serve to predict impacts to the program that could be detrimental to success. Thus, given that the design is acceptable from a safety and health perspective, a PRA for operations can focus on those aspects of risk that relate to system operability and maintenance and the performance of the mission. Risk importance measures determined by the PRA can be used to optimize procedures and resource allocations during operation.