NASA Procedural Requirements

NPR 8705.5
Effective Date: July 12, 2004
Expiration Date: March 12, 2010

COMPLIANCE IS MANDATORY

Probabilistic Risk Assessment (PRA) Procedures 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 REFERENCES
P.5 CANCELLATION

CHAPTER 1: Overview

1.1 Introduction
1.2 When to Use PRA
1.3 Documenting PRA Decisions
1.4 Implementation Responsibility

CHAPTER 2: PRA Process

2.1 Introduction
2.2 Definition of Objective(s)
2.3 System Familiarization
2.4 Identification of Initiating Events
2.5 Scenario Modeling
2.6 Failure Modeling
2.7 Quantification
2.8 Uncertainty Analysis
2.9 Sensitivity Analysis
2.10 Ranking
2.11 Data Analysis

CHAPTER 3: PRA Development Requirements

3.1 PRA Team
3.2 PRA Implementation
3.3 PRA as a Living Tool
3.4 PRA Quality
3.5 Independent Peer Review

CHAPTER 4: Application of PRA

4.1 General Requirements
4.2 PRA throughout the Life Cycle Phases

Appendix A: Acronyms

Preface

P.1 PURPOSE

This NPR provides basic requirements for performing a probabilistic risk assessment (PRA) for a NASA program or project. It addresses technical and safety risk and does not address programmatic risk involving consideration of cost and schedule.

P.2 APPLICABILITY

a. This NPR applies to NASA Headquarters and NASA Centers, including Component Facilities, and the Jet Propulsion Laboratory and service providers to the extent specified in their contracts with NASA.

b. This NPR shall be used specifically for programs/projects that provide aerospace products or capabilities; i.e., space and aeronautics systems, flight and ground systems, technology demonstration/validation, and operations (Requirement 32944).

c. This NPR is not required for other projects (such as research and technology development, training, or education); however, the PRA concepts and practices described within this document can be beneficial to other projects, so its application should be considered. The importance and scope (potential affects on public and worker safety, NASA significance, strategic importance, or schedule criticality) of the project/program being assessed is used to identify the extent of the risk assessment application.

d. The applicability of this NPR for projects/programs that are already in progress depends on the criticality of the risk assessment to project/program risk management, the feasibility of compliance, and the extent of the completion of the project/program. Decisions concerning applicability for projects/programs in progress will be made on a case-by-case basis involving program/project manager recommendations to the Governing Program Management Committee, which shall have approval authority (Requirement 32947).

P.3 AUTHORITY

a. 42 U.S.C. 2473(c)(1), Section 203(c) (1) of the National Aeronautics and Space Act of 1958, as amended.

b. NPD 8700.1, NASA Policy for Safety and Mission Success.

P.4 REFERENCES

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

c. NPR 1000.3, The NASA Organization.

d. NPR 1441.1, NASA Records Retention Schedule.

e. NPR 7120.5, NASA Program and Project Management Processes and Requirements.

f. NPR 8000.4, Risk Management Procedural Requirements.

g. NPR 8715.3, NASA Safety Manual.

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

P.5 CANCELLATION

None.

/s/ Bryan O'Connor

Associate Administrator for
Safety and Mission Assurance

DISTRIBUTION:

NODIS

CHAPTER 1: Overview

1.1 Introduction

1.1.1 It is NASA policy to implement structured risk management (RM) processes and use qualitative and quantitative risk assessment techniques to support optimal decisions regarding safety and the likelihood of mission success. This requirement is stated in NPD 8700.1, NASA Policy for Safety and Mission Success.

1.1.2 Probabilistic Risk Assessment (PRA) is a comprehensive, structured, and logical analysis methodology aimed at identifying and assessing risks in complex technological systems. PRA is generally used for low-probability, high-consequence events for which limited statistical data exist. Its application, as discussed in this document, is targeted at risk environments common within NASA that may involve the compromise of safety, inclusive of the potential loss of life, personal injury, and loss or degradation of high-value property that may be found in NASA mission-related programs.

1.1.3 PRA has become a principal analytical methodology for identifying and analyzing technical and safety risk associated with complex systems, projects, and programs. PRA facilitates RM activities by identifying dominant contributors (those events that contribute most to risk) so that resources can be allocated to significant risk drivers and not wasted on items that insignificantly affect overall system risk.

1.1.3.1 PRA provides a framework to quantify uncertainties in events that are important to system safety. By requiring the quantification of uncertainty, PRA informs the decision-makers of the sources of uncertainty and provides information that helps determine the worth of investing resources to reduce uncertainty.

1.1.3.2 PRA differs from reliability analysis in three important respects: (1) PRA tends to focus on the evaluation of system failure while reliability analysis tends to focus on the evaluation of system success; (2) PRA explicitly quantifies uncertainty while reliability analysis nominally considers uncertainty in parameter estimates; and (3) PRA quantifies metrics related to the occurrence of highly adverse consequences (e.g., fatalities, illness, loss of mission), as opposed to narrower system performance metrics such as system reliability. PRA also differs from hazard analysis, which evaluates metrics related to the effects of high consequence and low probability events, treating them as if they have already occurred; i.e., without regard to their likelihood of occurrence. PRA results are directly applicable to resource allocation and other kinds of RM decision-making based on its broader consequence metrics.

1.1.3.3 The PRA process identifies weaknesses and vulnerabilities in a system that can adversely impact safety, performance, and mission success. This information in turn provides insights into viable RM strategies to reduce risk and directs the decision-maker to areas where expenditure of resources to improve design and operation may be more cost-beneficial.

1.1.3.4 The most useful applications of PRA have been in the evaluation of complex systems subject to low-probability and high-consequence scenarios and the evaluation of complex scenarios consisting of chains of events, each of which may adversely impact the system. These complex scenario impacts may include events that separately may appear to be slight or insignificant but collectively can combine and interact to cause high severity consequences.

1.1.4 All PRAs shall be conducted in accordance with this NPR (Requirement 32960).

1.1.4.1 This NPR provides the basic requirements for use of PRA in NASA programs and projects.

1.1.4.2 A companion document to this NPR, the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf, provides further details on PRA methodology for aerospace applications. Many references will be made to this companion document for practical advice on performing PRAs.

1.2 When to Use PRA

1.2.1 NASA program and project managers shall use the criteria in paragraph 1.2.3, Table 1, and paragraph 1.2.4 to determine when a PRA must be conducted and the scope to be implemented (Requirement 32964).

1.2.2 The PRA approach for each project shall be described in the project's risk management plan and submitted for Governing Program Management Committee (GPMC) review and approval at the project formulation decision milestone (Requirement 32965).

1.2.3 Levels of PRA

1.2.3.1 Full Scope PRA

1.2.3.1.1 A "full-scope" analysis contains all major PRA components as outlined in chapter 2 of this NPR. Decision-making for projects involving complex systems in high-stakes programmatic contexts shall be supported by a full-scope PRA with consideration of uncertainty (Requirement 32969).

1.2.3.1.2 Full-scope PRAs address all applicable end states that lead to failure to meet safety and mission objectives. These end states include, but are not limited to, loss of crew, when a crew is part of the mission; accidental exposure to toxic or hazardous materials leading to potential illness or death of public or ground- or space-based personnel; loss of ground-based facilities; loss of space-based facilities or modules; mission abort; loss of mission; and mission reconfiguration.

1.2.3.1.3 Completeness of scenarios is an important consideration in a full-scope PRA. Uncertainty analysis shall be 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 (Requirement 32972).

1.2.3.2 Limited-Scope PRA

1.2.3.2.1 A "limited-scope" PRA applies the steps outlined in chapter 2 of this NPR with the same general rigor as a full-scope PRA but focuses on some of the mission-related end states of specific decision-making interest, instead of all applicable end states.

1.2.3.2.2 The scope is limited and is defined on a case-by-case basis, so that the results can provide specific answers to pre-identified mission-critical questions and safety concerns, rather than the assessment of all relevant risks.

1.2.3.2.3 Similar to a "full-scope" PRA, sources of uncertainties that have a strong effect on the limited-scope PRA results and insights shall be identified and quantified (Requirement 32976).

1.2.3.3 Simplified PRA

1.2.3.3.1 A "simplified" PRA applies essentially the same process outlined in chapter 2 of this NPR but identifies and quantifies major (rather than all) mission risk contributors (to all end states of interest) and generally applies to systems of lesser technological complexity or systems having less available design data than those requiring a full-scope PRA. Thus, a simplified PRA contains a reduced set of scenarios or simplified scenarios designed to capture only essential, sometimes top level, mission risk contributors.

1.2.3.3.2 In a simplified PRA, the sources of uncertainties that have the strongest effects on the PRA results shall be identified and, in cases where they affect the management decision process, shall be quantified (Requirement 32979).

Table 1. Criteria for Selecting the Scope of a Probabilistic Risk Assessment (PRA)

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE
Human Safety and Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return Missions	**F**
		White House Approval (PD/NSC-25)	Nuclear Payloads (e.g., Cassini, Ulysses, Mars 2003)	**F**
		Space Missions with Flight Termination Systems	Launch Vehicles	**F**
	Human Space Flight		International Space Station	**F**
			Space Shuttle	**F**
			Human Space Experiments	**F**
			Project Constellation	**F**
Mission Success (for non?human rated missions)	High Strategic Importance / High Value Strategic Property / High Cost Projects		Mars Program	**F**
	High Schedule Criticality		Launch Window (e.g., planetary missions)	**F**
	All Other Missions		Earth Science Missions (e.g., EOS, QUICKSCAT, specific payloads)	**L/S**
			Space Science Missions (e.g., SIM, HESSI, specific payloads)	**L/S**
			Technology Demonstration/Validation (e.g., EO-1, Deep Space 1)	**L/S**
			Medium to Low Cost Projects	**L/S**

*Key:

F - Full scope PRA as defined in paragraph 3.2.1.

L/S - Limited-scope or simplified PRA should be performed or altogether waived, at the direction of the program/project, as defined in paragraph 3.2.2 and 3.2.3.

1.2.4 Factors to Consider Regarding the Level of PRA.

1.2.4.1 Unlike a full-scope PRA, the complete set of scenarios is not of essence in either a limited-scope or a simplified PRA.

1.2.4.2 Considerations of program risk associated with schedule, performance, technology, and cost should be included for both full- and limited-scope PRAs but, perhaps, in separate analyses.

1.3 Documenting PRA Decisions

1.3.1 After determining the level at which the PRA shall be conducted, the program or project manager shall document the PRA decision and its basis in the program/project risk plan (Requirement 32984).

1.3.2 The program or project manager shall brief the GPMC on the PRA decision and the rationale during the formulation phase of the program or project (Requirement 32985). (See NPR 1000.3, The NASA Organization, paragraph 6.6.)

1.3.3 Any disputes concerning the PRA decision and level of implementation shall be elevated to the next level of Program Management Committee (Requirement 32986).

1.4 Implementation Responsibility

1.4.1 Enterprise Associate Administrators

1.4.1.1 NPD 8700.1, NASA Policy for Safety and Mission Success, states that Enterprise Associate Administrators and program/project managers are responsible for assuring that appropriate Agency safety, reliability, maintainability, quality, and RM policies, plans, techniques, procedures, and standards are implemented.

1.4.1.2 Towards that end, Enterprise Associate Administrators shall:

a. Ensure that appropriate resources (funding, personnel, methods, and software applications) are made available for PRA (Requirement 32991).

b. Ensure that technical quality is maintained throughout the PRA effort (Requirement 32992).

c. Ensure that PRA methodology and results are effectively transferred to appropriate NASA personnel who are not directly involved in conducting the PRA (Requirement 32993) .

d. Ensure that formal PRA awareness training and methodology training are provided periodically to managers and practitioners (Requirement 32994).

e. Ensure that PRA requirements are appropriately implemented on contracts (Requirement 32995).

1.4.2 Associate Administrator for Safety and Mission Assurance

1.4.2.1 The Associate Administrator for Safety and Mission Assurance is the lead for PRA policy, procedures, guidelines, technical training content, and tools throughout NASA. The Associate Administrator for Safety and Mission Assurance will continually evaluate and adopt best available PRA methods, practices, applications, software, and standards for use in NASA PRA efforts.

1.4.2.2 Further, the Associate Administrator for Safety and Mission Assurance shall:

a. Develop, coordinate, publish, disseminate, explain, interpret, and maintain NASA PRA policy and procedures and assure their correct implementation at Headquarters and at the Centers (Requirement 32999).

b. Have primary responsibility for developing criteria and guidelines for the use of PRA results in management decision-making (Requirement 33000).

c. Provide PRA functional leadership, mentoring, technical direction, and consultation on methodology (on how to conduct a PRA), tools, and oversight Agencywide (Requirement 33001).

d. Provide corporate leadership and establish a community of practice for the exchange of PRA-related information, best practices, and lessons learned across programs/projects, Centers, government agencies, and international partners (Requirement 33002) .

e. Assess and assure that PRAs are correctly initiated, conducted, and utilized within Enterprises and programs/projects (Requirement 33003).

f. Enable, facilitate, and organize the development of a PRA "corporate memory" (Requirement 33004). This includes:

(1) Assist in the maintenance of PRAs and their updating, as necessary (Requirement 33005).

(2) Collect, from NASA programs/projects, documentation of all PRAs conducted, including their scope, PRA models developed and data used, preliminary and final reports issued, and the results of independent or peer reviews (Requirement 33006).

(3) Assure the availability of all approved PRA documentation for present and future programs/projects (Requirement 33007).

g. Designate and provide or assist in acquiring state-of-the-art and verified PRA methods, computer applications, and training for NASA personnel (Requirement 33008).

h. Organize and coordinate peer reviews of PRA work performed, if deemed appropriate, and assure the implementation of peer review recommendations and the overall credibility of PRA efforts and results (Requirement 33009).

i. Contribute to and approve program/project Level 1 (NASA Headquarters-level program management) probabilistic risk assessment requirements; and provide oversight and advice on Level 2 (NASA Center-level program management) and lower-level probabilistic risk assessment requirements (Requirement 33010).

j. Assure that PRA results are provided in an acceptable, useable form (e.g., medians, means, lower and upper uncertainty bounds, and risk drivers) and are accurately represented and communicated to NASA management (Requirement 33011).

k. Guide and direct the use of PRA during the system development life cycle to improve design, operation, and upgrade (Requirement 33012).

l. Enable, facilitate, and organize a central resource and repository of PRA tools, methods, and data, and the transfer of PRA technology to NASA Civil Service personnel (Requirement 33013).

m. Assist in the acquisition and verify the credentials of PRA practitioners, both for Civil Service personnel and for supporting contractors or consultants (Requirement 33014).

1.4.3 Center Directors shall ensure that their Safety and Mission Assurance (SMA) and Engineering organizations acquire and maintain expertise in PRA necessary to support Center-based programs/projects (Requirement 33015).

1.4.4 Center Directors, Center SMA Directors, and program/project SMA Directors shall assist Center-based programs/projects in conducting required PRAs; i.e., provide required resources, training, tools, technical

advice, or assistance in obtaining competent support services (Requirement 33016).

1.4.5 Program/project managers and other decision-makers shall conduct and use PRA with the best state-of-practice methods and data to support management decisions to improve safety and performance (Requirement 33017). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapters 7 and 12.)

1.4.5.1 Program/project managers shall document PRA decisions, justifications and plans for implementing and conducting PRAs in program/project risk management plans (Requirement 33018).

1.4.5.2 The program or project manager shall brief the GPMC on the PRA decision and the rationale during the formulation phase of the program or project (Requirement 33019).

1.4.5.3 Program/project managers shall maintain and safeguard records resulting from PRAs in accordance with the guidelines in NPR 1441.1, NASA Records Retention Schedule ((Requirement 33020).

1.4.5.4 Program/project managers shall adequately and clearly communicate PRA results and insights that explicitly include initial assumptions, residual uncertainties, and significant risk drivers to all involved program/project staff and management, and ensure that the PRA results and insights, as well as their implications regarding systems design, operation, and upgrade, are reviewed, analyzed, properly interpreted, and understood (Requirement 33021). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

1.4.5.5 Program/project managers shall update design, operating, and implementation plans to reflect insights from PRA and use the insights gathered from PRA to reinforce or modify existing relevant management decisions or to generate new management decisions (Requirement 33022). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

1.4.5.5.1 If the residual risk, as shown through the use of PRA, is deemed unacceptable as defined by program requirements, the program/project manager shall consider modifying the project through design, operation, upgrade, and maintenance, and implement management decisions to reduce risk to an acceptable level as defined at the appropriate level of the Agency; i.e., Headquarters, Center, Enterprise, program, or project, as appropriate (Requirement 33023).

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

1.4.6 NASA shall, through prudent hiring, professional development, and mentoring, increase and maintain its capability to conduct, understand, and use PRA in support of a program/project life cycle (Requirement 33025).

CHAPTER 2: PRA Process

2.1 Introduction

>2.1.1 PRA characterizes risk in terms of three basic questions: (1) What can go wrong? (2) How likely is it? (3) What are the consequences? The PRA process answers these questions by systematically postulating and quantifying undesired scenarios in a highly integrated fashion. The process uses a collection of models based on systems engineering, probability theory, reliability engineering, physical and biological sciences, and decision theory.

2.1.2 The process that shall be used for conducting a typical scenario-based PRA involves objective definition, system familiarization, identification of initiating events, scenario modeling, failure modeling, quantification, uncertainty analysis, sensitivity analysis, importance ranking, and data analysis (Requirement 33029). The following paragraphs provide a top-level overview of the process for conducting a typical scenario-based PRA. It is recognized that some deviations from the techniques summarized below may be necessary as long as the adopted techniques are based on proven and accepted methods and analytical tools.

2.1.3 The process and techniques provided in the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners shall be used for conducting PRAs in accordance with this NPR (Requirement 33031). In addition, the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners cites references that provide more detailed information concerning the PRA process. (Two examples of PRAs are provided in chapter 15 of the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners.)

2.2 Definition of Objective(s)

2.2.1 The first, and perhaps the most important, step in a PRA is to clearly and unambiguously state the study objective(s). Without this step, the rest of the assessment will be either incomplete or inadequate and, therefore, a waste of time, money, and effort. The objective of the risk assessment shall be well defined and, associated with it, the appropriate undesirable consequences of interest (called "end states") that are consistent with the stated study objective(s) must be identified and selected (Requirement 33035). These consequences may include harm to humans (e.g., injury, illness, or death), degradation of mission capabilities, loss of mission, property losses, or other consequences for which appropriate metrics must be selected. In NASA, these undesired end states are generally classified as mishaps.

2.2.2 Depending on the scope of the PRA, applicable configuration, time frame, and rules for considering initiators (i.e., whether to include external events such as micrometeoroids) shall be defined (Requirement 33037). Ground rules for both scope and detail should be developed and reviewed by the project manager and cognizant SMA organization. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapters 2 and 3.)

2.3 System Familiarization

Familiarization with the entity system(s) under analysis is the next step. This activity covers the review of all relevant design and operational information, including engineering and/or process

drawings, as well as operating, emergency, and maintenance procedures. If the PRA is performed on an existing system that has been operated for some time, the engineering information shall be on an as-built and as-operated basis; if the PRA is conducted on a new or proposed system, then the as-designed system shall be used as the basis(Requirement 33040). Visual inspection of the system being analyzed is strongly recommended and should be conducted to the extent possible. The purpose of this step in the analysis is to make the analyst(s) thoroughly familiar with the system and its design and/or operation, and to gain an understanding of the success states (conditions or parameters of success) needed for proper operation. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 6.)

2.4 Identification of Initiating Events

2.4.1 The complete set of initiating events (see Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, sections 15.1.7/8 and 15.2.5) shall be identified (Requirement 33043).

2.4.1.1 An initiating event is the beginning of an accident "scenario." It is an event that triggers subsequent chains of events.

2.4.1.2 The initiating events shall be identified, analyzed, and screened to ensure that they have the potential to initiate accident scenarios leading to the defined end states (Requirement 33045). Initiating events leading to a set of scenarios that have the same end state but having very low probabilities can be screened out.

2.4.1.3 The identification of the initiating events can be accomplished with special types of top-level logic trees (see Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, section 15.1.12), called master logic diagrams (see Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, section 15.1.6). Additional techniques, like Failure Modes and Effects Analysis (see NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy, and NPR 8715.3, NASA Safety Manual) can also be used to identify initiators. Independent initiating events can then be grouped according to the similarity of challenges that they pose to the system (system responses that result from their occurrence). When initiating events are treated as a group, their frequencies shall be logically summed up to derive the group initiator frequency (Requirement 33048). (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapters 4, 5, and 15.)

2.4.2 In some projects/programs, mission phases and durations are well defined (e.g., launch, ascent, orbit, descent). In these situations, it may be advantageous to initiate PRA scenarios with a successful mission initiator (e.g., launch) and/or mission phase transition (e.g., first stage separation) instead of a detrimental initiating event as described above.

2.5 Scenario Modeling

The PRA shall identify and evaluate potential scenarios leading to undesired consequences (Requireme (Requirement 33050). The modeling of each accident scenario is an inductive process that usually involves graphical and logical tools/techniques called event trees. An event tree starts with the initiating event and progresses through the scenario, a series of successes or failures of intermediate events (also called pivotal events or top events), until end states are reached. The binary logic option of success or failure is usually employed at each branch point of an event tree. Sometimes, a graphical tool called an event sequence diagram (ESD) is first used to describe an accident scenario, because this type of diagram lends itself better to engineering thinking than does an event tree. An

ESD is converted to an event tree for quantification. Other types of inductive modeling tools can also be employed. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapters 6, 8, and 10.)

2.6 Failure Modeling

The PRA shall evaluate the failure (type and probability) of each event in the scenarios identified above (Requirement 33052). The modeling of the failure causes (or their complements, successes) of each pivotal event or event tree top event is a deductive process that usually involves tools called fault trees. A fault tree consists of three parts. The top part is the top event, which corresponds to the failure of a pivotal event (or event tree top event) in the accident scenario. The middle part consists of intermediate events (faults) causing failure of the top event. These events are linked through logic gates (e.g., AND gates and OR gates) to the bottom part of the fault tree, the basic events, whose failure ultimately causes the top event to occur. The fault trees are then linked to the accident scenarios and simplified (using Boolean reduction rules) to support quantification. Other deductive modeling tools can be employed to evaluate the failure of top events, and alternative fault tree quantification techniques (e.g., binary decision diagrams) can also be used. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 10.) The combination of the inductive logic of event trees with the deductive logic of fault trees is a very powerful asset in PRA scenario modeling.

2.7 Quantification

The PRA shall quantify the scenarios (Requirement 33054). Quantification refers to the process of estimating the frequency and the consequences of the undesired end states. The frequency of occurrence of each end state is calculated using a fault tree linking approach resulting in a logical product of the initiating event frequency and the (conditional) probabilities of each pivotal event along the scenario path from the initiating event to the end state. The fault trees for each pivotal event are linked to the event tree to quantify the pivotal events in terms of the basic events. All like end states are then grouped; i.e., their probabilities are logically summed into the probability of the representative end state. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 10.)

2.8 Uncertainty Analysis

Because PRA attempts to model uncertain events (events that exhibit variability that cannot be eliminated), the risk model is, in essence, an uncertainty analysis model. Recognition of uncertainty analysis as the fabric of the PRA model is paramount to proper application of PRA results in the RM decision-making process. PRA analysts find ways to quantify and present the uncertainty associated with risk results in a manner that is understandable to decision-makers. Any PRA insights reported to decision?makers shall include an appreciation of the overall degree of uncertainty about the results and an understanding of which sources of uncertainty are critical(Requirement 33057). Presentation of PRA results without uncertainties significantly detracts from the quality and credibility of the PRA study. Monte Carlo simulation methods (or other related methods; e.g., the Latin Hypercube method) are generally used to perform uncertainty analysis on a PRA. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 12.)

2.9 Sensitivity Analysis

Sensitivity analysis is a type of uncertainty analysis that focuses on modeling uncertainties in assumptions, models, and basic events. These analyses are frequently performed in a PRA to indicate those analysis inputs or elements whose value changes cause the greatest changes in partial or final risk results. A sensitivity analysis is aimed at evaluating result changes due to postulated input parameter changes. This type of analysis is often performed to determine which input parameters in a PRA are most important and deserve the greatest attention and need for improvement. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

2.10 Ranking

One of the most important products of a PRA is the relative importance of the calculated risks. Therefore, special importance measures, such as Fussel-Vesely, Risk Reduction Worth (RRW), Birnbaum, Risk Achievement Worth (RAW), and differentials, are used to identify the lead, or dominant, contributors to risk in accident sequences or scenarios. The listing of these lead or dominant contributors in decreasing order of importance is called importance ranking. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

2.11 Data Analysis

The PRA shall conduct data analyses to support quantification (Requirement 33061). Data analysis refers to the process of collecting and analyzing information in order to estimate various parameters of the PRA models. These parameters are used to obtain probabilities of the various events including component failure rates, initiator frequencies, and human and software failure probabilities. Developing a PRA database of parameter estimates involves: (1) identification of the data needed; (2) data collection; and (3) parameter estimation using statistical methods to develop uncertainty distributions for the model parameters. In cases where there are no statistically significant data to support PRA parameter estimation, the PRA analyst may need to rely on expert judgment and elicitation. The data analysis task proceeds in parallel or in conjunction with the steps described above. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapters 8, 9, 10, and 11.)

CHAPTER 3: PRA Development Requirements

3.1 PRA Team

3.1.1 A multi-disciplinary team representing all key functional elements (e.g., design, engineering, operation, system safety, and maintenance) and appropriate NASA organizations is best qualified to perform the PRA.

3.1.1.1 The PRA should factor in the impacts of inter- and intra-project or mission dependencies.

3.1.1.2 The PRA should use and incorporate the insights offered by workers and crew. The goal is to develop an objective or "unbiased" risk model.

3.1.2 The PRA team shall include a PRA expert who has had training and extensive experience in the application and conduct of PRAs, preferably for several different types of systems. The PRA expert shall serve as the PRA Technical Authority, with technical decision-making authority for the PRA (Requirement 33068). This is particularly important for teams with personnel drawn from many organizations or for teams without extensive practical PRA experience.

3.1.2.1 The PRA Technical Authority shall guide or facilitate the process and keep Headquarters Office of Safety and Mission Assurance informed of PRA activities and status (Requirement 33070).

3.1.2.2 Selection of the PRA Technical Authority shall be made with guidance from Center SMA organizations or Headquarters Office of Safety and Mission Assurance (Requirement 33071).

3.2 PRA Implementation

Several items should be considered when implementing and developing a PRA. These items include gaining an understanding of the state-of-practice in PRA applications, establishing the scope of the analysis, defining terminology, determining methods to be used to evaluate scenarios, collecting and analyzing data, identifying and analyzing major risk contributors, and participating in an independent peer review of the PRA results.

3.2.1 Scope the level of detail in a PRA to be commensurate with the mission phase, complexity of the systems, severity of the hazards, the objective/scope of mission/project (e.g., tailored approach), and the maturity of the design being analyzed.

3.2.2 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. Terminology shall also be consistent with what is used in the program/project in order to facilitate risk communication (Requirement 33075).

3.2.3 Identify major contributors to risk as outlined in chapters 2 and 3 and as described in Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. Contributors to undesired events shall be quantified on the basis of existing data (Requirement 33077). This requires that some analyses of previous mission failures be performed. (See Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 13.)

3.2.4 Determine the types of analyses that shall be performed for each scenario. Analyses should include appropriate state-of-practice PRA modeling techniques. (See chapter 3 and Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 15.)

3.2.5 Review for adequacy existing generic or specific risk databases intended for use in PRAs. Guidance on the use of data for PRAs is given in the Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, chapter 8. These databases may need to be modified or enhanced depending on the systems or environments being modeled.

3.2.6 Review the status of ongoing PRAs periodically and determine the continued adequacy of these analyses, their models, and their results. For important programs or projects, the credibility of the PRA will be enhanced by an independent peer review (see paragraph 4.5 below).

3.3 PRA as a Living Tool

3.3.1 PRAs generally provide risk assessment snapshots in time. Therefore, they can become obsolete if they are not reevaluated and updated periodically to reflect design and operational changes. The periodic reevaluation and updating of a PRA will provide the user with a "living" or periodically updated risk assessment tool of added value.

3.3.2 Another interpretation of the term "living PRA" is as a "risk monitor." It is a modification of the PRA model and analysis to allow rapid calculations to support management decisions in real time. The purpose of this capability is to support timely operational RM to help ensure that system operation, maintenance, and testing configurations pose minimal or acceptable risk.

3.4 PRA Quality

3.4.1 A PRA shall follow quality assurance principles and practices that are analogous to those in other engineering fields and practices (Requirement 33085). These principle and practices include the following:

a. Selection of a suitable PRA project team, with appropriate PRA training, experience, and expertise, that is knowledgeable about the project/program being assessed, consistent with project objective(s) and the level and scope of the PRA as discussed in chapters 2 and 3 of this NPR.

b. Proven and accepted methods and analytical techniques and tools that fit the specific application.

c. Proven, verified, validated, and widely accepted computer programs with user manuals that are adequately documented to minimize opportunities for error and inappropriate use.

d. Common assumptions and ground rules agreed to at the start of the PRA and updated/maintained as the PRA effort progresses.

e. Clear technical procedures and guidance based on the selected methods, analytical tools, and computer programs.

f. Engineering (design and operation) and analysis data (e.g., reliability) collected and processed to meet the needs of the project.

g. Sound management direction and practices to allow performance of the tasks during allowable, yet realistic schedules.

h. Coordination, communication, compatibility, and centralized leadership of the PRA efforts

involving distributed teams; e.g., at different Centers.

i. Adequate internal review and documentation.

j. Effective interfaces with engineering staff and management to exchange information and provide inputs and review.

k. Adequate time, opportunity, and environment for incorporating improvements.

l. A strong tie with program/project configuration and requirements management activities to ensure that the PRA being developed reflects the latest or the most suitable design.

3.4.2 Consider and implement these principles and practices to maximize the likelihood of a successful PRA.

3.5 Independent Peer Review

3.5.1 In order to enhance the quality and credibility of a PRA study, an independent peer review of the work shall be conducted for all full-scope PRAs (Requirement 33101) and should also be conducted for all other PRAs.

3.5.1.1 This review shall be carried out by independent peers, that is, recognized PRA experts who are not involved in the study and have no stake in it (Requirement 33102).

3.5.1.2 The peers' expertise should span the range of disciplines and experience required for the study.

3.5.1.3 In general, this review shall concentrate on the appropriateness of methods, information, sources, judgments, and assumptions as well as their application to the program/project/system being evaluated and its objective(s) (Requirement 33104).

3.5.2 The use of a participatory peer review should be considered. This is a peer review process that begins early and proceeds in parallel with the project involving frequent, periodic contact and interactions with the PRA team in order to identify problems and to recommend corrective actions early, instead of waiting to begin the peer review when the PRA is virtually complete. While this approach may sacrifice some independence in the peer review, it is likely to result in a PRA performed correctly the first time, saving expenditure of time and resources to correct problems at the end of the project.

CHAPTER 4: Application of PRA

4.1 General Requirements

4.1.1 A PRA shall be comprehensive, balanced, and tailored (Requirement 33108).

4.1.1.1 A comprehensive PRA shall consider the complete environment and all factors that pertain to the system being assessed, including, as appropriate to satisfy its stated objective(s), the safety of the public, astronauts, pilots, and the NASA workforce; protection of high-value equipment and property; adverse impacts on the environment; national interests; and security (Requirement 33109).

4.1.1.2 A balanced PRA shall ensure that the scope considers issues of safety, operation, and mission assurance; is conducted at a level commensurate with the level of risk; and is timely to assist program/project management in limiting risk (Requirement 33110).

4.1.1.3 A tailored PRA shall ensure that the level of detail is commensurate with the complexity of the hazards, scope, and objective(s) of the mission/project being evaluated (Requirement 33111).

4.1.2 PRA implementation procedures shall reflect and incorporate the results of project risk analysis (Requirement 33112), including:

a. Identification of the elements of risk (initiators, hazards, scenarios, probabilities, and consequences) (Requirement 33113).

b. Recommended controls (preventive and mitigating features, compensatory measures) needed to reduce and manage risks (Requirement 33114).

4.2 PRA Throughout the Life Cycle Phases

A common misconception is that a PRA is not possible or useful when few data are available. In fact, this is precisely the situation when a PRA is most useful. The comprehensive and systematic nature of the assessment associated with a PRA is directly applicable to systems with the largest uncertainties. No PRA would be needed if all information required to ensure mission safety is known with certainty. Although a PRA is useful in all program/project life cycle phases, the type of information that is required and the types of scenarios modeled vary. This is illustrated in the following discussion of a typical program/project life cycle consisting of four phases: design, operation, upgrade, and decommissioning. This discussion demonstrates that, in all these phases, the assessment of comparative or relative risk, rather than its absolute value, will be most useful.

4.2.1 PRA in Design

Design generally seeks to optimize programs, missions, and/or systems to meet required objectives and functionality within technical, schedule, regulatory, and cost constraints. A good design effort generally develops technologically feasible configurations that meet required objectives and seeks options that best satisfy schedule and regulatory constraints while minimizing costs. PRAs are used to identify and quantify the risks associated with each option for input to management trade-off processes that include minimizing risk. Even if mission specific data do not exist, failure rates and failure probabilities can be bracketed by comparisons with components where data do exist. When specific data do not exist, expert judgment data based on sound expert elicitation processes can be used to estimate top-level relative risk conclusions. Risk importance measures determined by a PRA

will also serve to focus the evolution of the design.

4.2.2 PRA in Operation

During operation, especially for new programs and missions, there are many questions related to the anticipated success of the program or mission. 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 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. A PRA for operations can also include performance considerations and regulatory requirements. If there are problems meeting performance or regulatory requirements, PRA can identify modifications to hardware, software, and operational parameters that may be the appropriate solutions.

4.2.3 PRA in Upgrade

After operating a system for a while, experience is gained and improvements may be required. In addition, changing technology, obsolescence of components, and aging will play significant roles in the need for improvement or upgrades to a system. To this end, a PRA can identify upgrade options that minimize risk. Generally each upgrade will have its advocates. PRA provides an assessment tool for evaluating the relative risk benefits of alternative upgrade options.

4.2.4 PRA at End of Life or in Decommissioning

When a product is at the end of its useful life, it is important that its end of operation and subsequent dismantling and disposal be conducted cost-effectively, with due consideration to regulatory requirements and regard to the safety of the surrounding population and environment. A PRA can be effectively used to assess dismantling, decommissioning, and disposal options that minimize risks. Transitioning to a replacement system can also be included in this category if the replacement system is drastically different from the system being replaced, or if the transition is terminal. If the replacement system is an improvement, transitioning can be included as an upgrade as described in paragraph 3.4.3.

Appendix A: Acronyms

GPMC	Governing Program Management Committee
EO-1	Earth Observing 1
EOS	Earth Observing System
ESD	Event Sequence Diagram
HESSI	High Energy Solar Spectroscopic Imager
NPR	NASA Procedural Requirements
NPD	NASA Policy Directive
PD/NSC-25	Presidential Directive/National Security Council Memorandum # 25
PRA	Probabilistic Risk Assessment
QUICKSCAT	Sea Winds Scatterometer Satellite
R&M	Reliability and Maintainability
RM	Risk Management
SIM	Space Interferometry Mission
SMA	Safety and Mission Assurance