NASA Procedural Requirements

NPR 8705.5
Effective Date: July 12, 2004
Expiration Date: July 12, 2009

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Subject: Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects

Responsible Office: Office of Safety and Mission Assurance

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.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | AppendixA | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS