



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[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [AppendixA](#) | [ALL](#) |

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 ([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.)

[| TOC](#) | [| Preface](#) | [| Chapter1](#) | [| Chapter2](#) | [| Chapter3](#) | [| Chapter4](#) | [| AppendixA](#) | [| ALL](#) |

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

DISTRIBUTION:

NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
