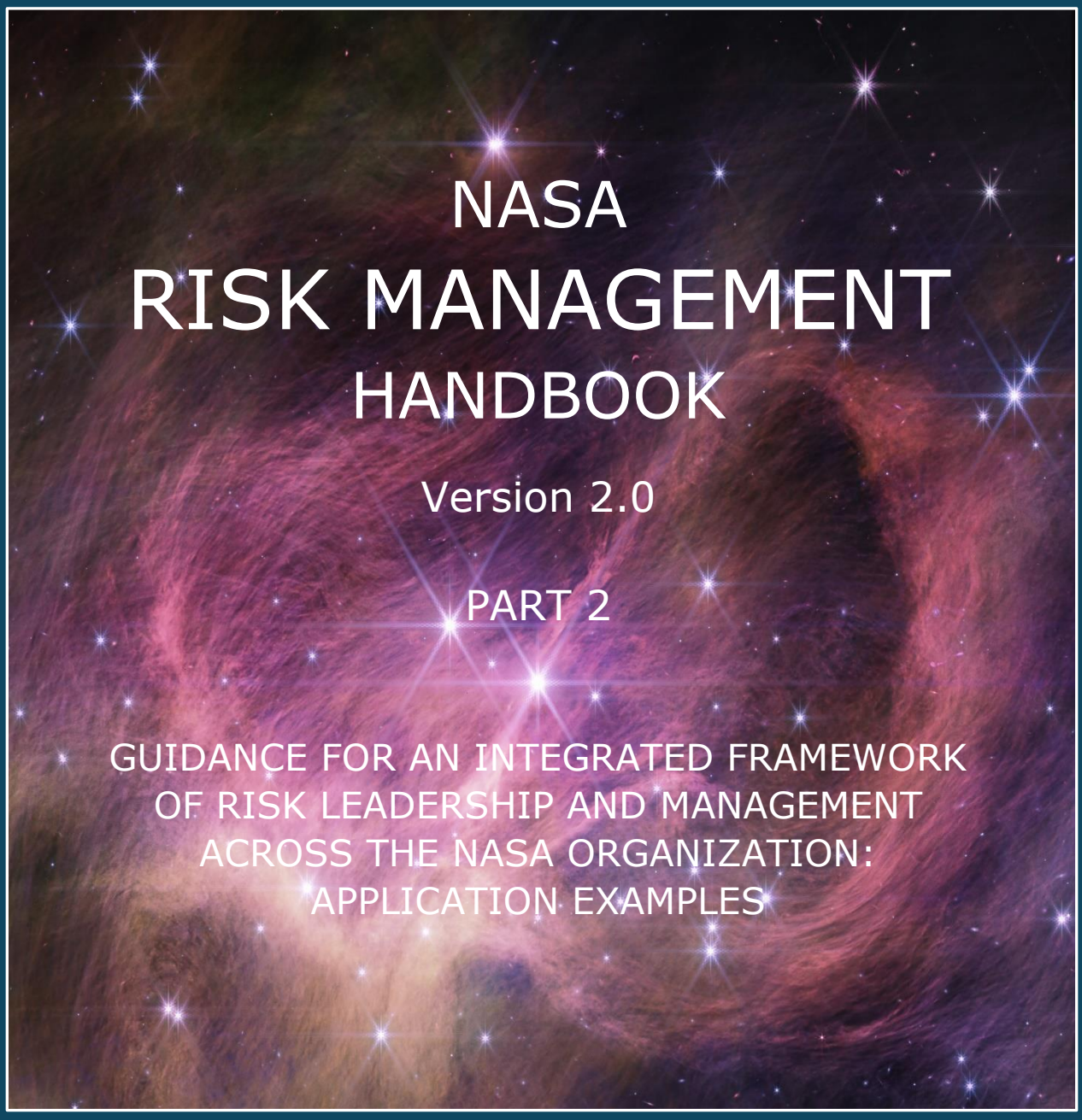
NASA/SP-20240014326
November 2024



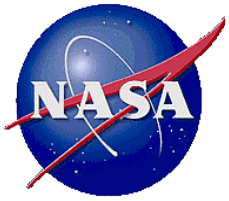
NASA
RISK MANAGEMENT
HANDBOOK

Version 2.0

PART 2

GUIDANCE FOR AN INTEGRATED FRAMEWORK OF RISK LEADERSHIP AND MANAGEMENT ACROSS THE NASA ORGANIZATION: APPLICATION EXAMPLES

www.nasa.gov



NASA/SP-20240014326

NASA SP-202400114326 and NASA SP-20240014019 supersede NASA SP-2011-3422 dated November 2011.

Cover image: Brown dwarf identified by James Webb Space Telescope in star cluster IC 348, about 1000 light-years away

Comments, questions, and suggestions regarding this document can be sent to:

Dr. Homayoon Dezfuli
NASA Technical Fellow
NASA Headquarters, Office of Safety and Mission Assurance (OSMA)
hdezfuli@nasa.gov or

Dr. Mary Coan Skow
Agency Risk Management Officer
NASA Headquarters, Office of Safety and Mission Assurance (OSMA)
mary.coan@nasa.gov

National Aeronautics and Space Administration
NASA Headquarters Washington, D.C. 20546
November 2024

ACKNOWLEDGMENTS

The authors express their gratitude to NASA's Leadership for their support and encouragement in developing this document, the second edition of the NASA Risk Management Handbook. Building upon the work that resulted in the first edition of this handbook, the development effort leading to this two-volume handbook was conducted in stages and was supported through reviews and discussions by the Agency Risk Management Working Group (ARMWG) and the Agency Risk Management Officer (ARMO) Team and by the Agency reviewers of the pre-publication version of the handbook. The authors also acknowledge the contribution of Michael Yau of ASCA Inc. to the development of this handbook.

AUTHORS:

Homayoon Dezfuli, NASA Headquarters

Sergio Guarro, ASCA Inc.

Chris Everett, Idaho National Laboratory

Allan Benjamin, Quality Assurance & Risk Management Services, Inc.

Mary Coan Skow, NASA Headquarters

REVIEWERS:

Reviewers who provided comments on the drafts leading up to this version are

Tahani Amer, NASA Headquarters

Wilma Anton, NASA Johnson Space Center

Dan Blackwood, NASA Goddard Space Flight Center

Willie Blanco, NASA Goddard Space Flight Center

Alfredo Colón, NASA Headquarters

Frank Fried, NASA Goddard Space Flight Center

Scott Graham, NASA Glenn Research Center

Christine Greenwalt, NASA Glenn Research Center

Danielle Griffin, NASA Glenn Research Center

Gene Griffith, NASA Langley Research Center

Marjorie Haskell, NASA Headquarters

Linda Hastings, NASA Glenn Research Center

Don Helton, NASA Headquarters

Steven Hirshorn, NASA Headquarters

Vicky Hwa, NASA Headquarters

Maggie Jones, NASA Headquarters

Prince Kalia, NASA Goddard Space Flight Center

Michele King, NASA Headquarters

Terry Lambert, NASA Glenn Research Center

Eric Miller, NASA Armstrong Flight Research Center

Wendy Morgenstern, NASA Headquarters

John Orme, NASA Headquarters

Ariel Pavlick , NASA Headquarters

David Payne, NASA Space Communications and Navigation

Kelli Peterson, NASA Glenn Research Center

Robin Ripley, Goddard Space Flight Center

Jeffrey Sheehy, NASA Headquarters

Virginia Stouffer, NASA Headquarters

Madelyn Suttle, NASA Marshall Space Flight Center

Sharon Thomas, NASA Johnson Space Center

Tim Trenkle, NASA Goddard Space Flight Center

Mike Viens, NASA Goddard Space Flight Center

Zion Young, NASA Ames Research Center

Contents

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

AE	Activity Execution
Ai	Alternative i
AoA	Analysis of Alternatives
AP-RIDM	Activity-Planning Risk-Informed Decision Making
ARMO	Agency Risk Management Officer
ARMWG	Agency Risk Management Working Group
BBN	Bayesian Belief Network
CCDF	Complementary Cumulative Distribution Function
CDF	Cumulative Distribution Function
CMLV	Commercial Medium-Lift Launch Vehicle
ConOps	Concept of Operations
CP	Cost of Project
CRM	Continuous Risk Management
DOE	Department of Energy
ESDR	Expert Staff Development Ratio
FCOM	Fraction [of Project] to Commercial Providers
FDOE	Fraction [of Project] to DOE
FPS	Fission Power System
FTE	Full-Time Equivalent
GAO	General Accounting Office
HEU	Highly Enriched Uranium
HLV	Heavy-Lift Launch Vehicle
HPM	Hybrid Procurement Model
HQ	Headquarters
ID	Influence Diagram
INSRB	Interagency Nuclear Safety Review Board
IT	Information Technology
IV	Independent Variable
KPM	Key Performance Measure
LOM	Loss of Mission
LOX	Liquid Oxygen
LV	Launch Vehicle
MD	Mission Directorate
MLV	Medium-Lift Launch Vehicle
MSD	Mission Support Directorate
MSO	Mission Support Office
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
NDP	NASA Development Policy
NEPA	National Environmental Policy Act
NHLV	NASA-Provided Heavy-Lift Launch Vehicle
NLM	Number of Launch Missions
NPD	NASA Policy Directive
NPP	NASA Procurement Policy

NPR	NASA Procedural Requirements
NPSPD	Nuclear Planetary Surface Power Delivery
NRE	Nuclear Reactor Enrichment
NRM	Nuclear Reactor Mass
NSPM-20	National Security Presidential Memorandum-20
NSSPFD	Nuclear Space System Procurement Framework Definition
ODRM	Objectives-Driven Risk Management
OIG	Office of Inspector General
OSMA	Office of Safety and Mission Assurance
PC	Probability of Contamination
PC	Project Cost
PCC	PC Constraint
PCR	PC Risk
pdf	Probability Density Function
P(LOM)	Probability of Loss of Mission
PLRA	Probability of Launch or Reentry Accident
PM	Performance Measure
PMK-G	Performance Goal
PMK-R	Performance Requirement
PMS	Probability of Mission Success
PRA	Probability Risk Assessment
PRR	Probability of Radiological Release
PRRC	PRR Constraint
PRRR	PRR Risk
PXNPB	Planet X Nuclear Power Base
QRTV	Quantitative Risk Tolerance Value
R&D	Research and Development
RIDM	Risk-Informed Decision Making
RM	Risk Management
RMP	Risk Management Plan
RNxxV	Risk Normalized Value of xx
RPM	Reactor Power Module
RPS	Radioisotope Power System
RSD	Risk Scenario Diagram
RTG	Radioisotope Thermoelectric Generator
RTL	Risk Tolerance Level
SA	System Assembly
SMD	Science Mission Directorate
SME	Subject Matter Expert
SMS	Safety and Mission Success
SSA	System Safety Analysis
STEM	Science, Technology, Engineering, and Math
STMD	Space Technology Mission Directorate
TLM	Transfer and Landing Module
TLR	Time to Launch Readiness
TLRC	TLR Constraint

TLRR	TLR Risk
TRL	Technology Readiness Level
U/U	Unknown and/or Underappreciated

1 Introduction

Part 2 of the Risk Management (RM) Handbook has as its primary objective an illustration of the concepts and processes introduced in Part 1, by means of examples of RM implementation in current or likely near-future contexts of National Aeronautics and Space Administration (NASA) activity. Throughout the discussion of the included set of examples, it also strives to provide perspective on the importance of understanding the close interconnections among the management of risk and the pursuit of the organizational objectives to which the application of RM processes applies. This introductory chapter provides a roadmap to the organization of the materials that are included in Part 2 to fulfill its illustration and exemplification goals.

For a NASA reader's perspective, it is noted that, although the examples of RM application presented throughout Part 2 are based on realistic premises and assumptions, they are nevertheless "fictional" and sometimes projected into the realm of space technology advances that are deemed possible in the not-so-far future, but that at the present time are yet to come. In any case, the definition of NASA mission and/or activity concepts and execution modes that are presented in the examples are under no circumstances to be interpreted as suggestions by the authors of this handbook for actual mission design and concepts of operations (ConOps) applicable to actual future NASA missions. Also, some of the examples address activities that, if actually undertaken, would involve the sharing of management and decision responsibility for certain aspects of the associated projects and missions between NASA and other Government entities (e.g., such as the U.S. Department of Energy, in the case of missions carrying nuclear power sources on board). The examples that discuss missions or project where such interfaces may apply are by no means to be interpreted as providing or prescribing definitions of the related interagency interactions and assignment of responsibilities. Such definitions may be the realm of government policies or regulations that this handbook is not intended to cover or discuss.

1.1 Intended Use of Part 2

The activities and projects that provide the basis and context of the RM application examples discussed in Chapters 2 thru 3 of this Part 2 reside within the three principal domains of RM application identified in Part 1 (more specifically in Part 1 Chapter 2), i.e.: the Enterprise, Program/Project, and Institutional domains. As stated above, while it is useful to keep in mind the distinct classification of activities according to the domain within which they are executed, this RM Handbook Part 2 places, in the presentation and discussion of the RM examples provided, attention and emphasis on the cross-organizational aspects of a coordinated and integrated approach to the management of risk and opportunity, in the pursuit of the related objectives.

Because they emphasize the need for, and benefits of, an integrated and cross-organizational implementation of RM, the Part 2 examples explicitly illustrate and discuss the continuity of application and interfacing of the Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM) processes, in their role of complementary foundational components of the overall NASA Objectives-Driven Risk Management (ODRM) framework.

In light of the above, the reader will find in the first portion of Part 2 explicit reference to the concepts introduced in Part 1 Chapter 2 with regard to how the connective tissue constituted by

the flow-down of organizational activity objectives across domains and organizational interfaces needs to be recognized and identified, so that a corresponding awareness and understanding of the interrelations among risks across and up-and-down the spectrum of affected activities can be developed by both managers and technical staff members at all levels of the organization. It is only with the achievement of such a broader awareness and understanding of the relationships among and across strategic and execution-level agency objectives that risk can be identified and managed from an integrated perspective, rather than been viewed solely viewing such risks uniquely from the stove-piped narrow angles of individual projects and organizational entities / units.

The remainder of Part 2, beyond the initial exemplification of ODRM principles relative to objectives and risk posture flow-down that is presented in Chapter 2, can be viewed and used as a spectrum of examples that address the risk management of activities and projects at different stages of their lifecycles. The examples are also presented at different levels of complexity to illustrate the principle of a graded approach to risk assessment and management, as discussed in Part 1. The reader can therefore see in the examples how ODRM processes and techniques may be tailored so that their analytical rigor and level of detail is commensurate to the risk postures that are being applied and to the type and quality of the information available to assess risk and make related risk-informed activity-management and project-management decisions.

A summary outline of the contents of the Part 2 individual chapters is provided in the following section.

1.2 Overview of Part 2 Contents and Organization

As stated above, before the discussion of RM implementation examples relative to specific activity or mission contexts, Part 2 provides examples illustrating the identification of RM objectives and associated plans, based on the flow-down of activity and project objectives from the top Enterprise Domain strategic level to the lower execution levels. As discussed at the concept level in Part 1 Chapter 2, such a flow-down branches out into the Program/Project Domain execution of projects and missions on one hand, and/or on the other hand into the Institutional Domain activities set up to fulfill cross-agency or project-specific institutional support needs. The examples in Part 2 Chapter 2 thus illustrate the principles and rationale for pursuing a coordinated and integrated implementation of RM processes according to the concepts introduced in Part 1 Chapter 2. These principles should remain well present in the reader's mind as a key to a better understanding and interpretation of the ODRM application examples provided in the following chapters of Part 2 (Chapters 3 and 4).

The discussion of ODRM implementation examples throughout Part 2 chapters is thus articulated along the following overall development lines:

Chapter 2 provides, as an example of overall RM context, a given flow-down of activity objectives, from a hypothetical but realistic Enterprise Domain strategic objective and associated high-level analysis of alternatives (AoA), into execution-level mission and institutional sets of objectives. Chapter 2 then proceeds to discuss the selection of RM processes of either the RIDM or CRM type, as suited to manage risk for the specific contexts of the enterprise, program/project, or institutional activities set up and executed to pursue the objectives produced by the flow-down process. It should be noted that the latter process is an external process complementary to RM and

its outcomes, i.e., the definition of the ensemble of organizational objectives and activities at all levels, is to be viewed and treated as a pre-established context within which RM plans and activities are to be accordingly defined.

Chapter 3 covers an example of "Activity-Planning" risk management execution, which typically consists of a risk-informed AoA based on RIDM processes. The example addresses the risk-informed selection of system-design and mission-design solutions at the onset of a specific Program/Project Domain life-cycle execution. The example includes the application of criteria for aligning the use of RIDM processes to the risk posture that is identified upfront, according to the type of information that is available for the assessment of risk – e.g., qualitative vs. quantitative data and information concerning the level of risk affecting an activity and its objectives.

Chapter 4 covers examples of CRM execution within a particular Project and within a particular Center. The risks analyzed and managed within the Project entity pertain to objectives identified in Table 4-I. The risks analyzed and managed within the Center pertain to project support objectives identified in Table 4-II and institutional objectives identified in Table 4-III and Table 4-IX. The CRM execution examples in Chapter 4 are presented at a level of breadth and depth that is intended to convey the guidance needed by skilled practitioners of CRM on a technical level. Topics covered include the development of risk statements, the analysis and classification of individual risk scenarios, the aggregation of individual risk scenarios affecting an objective, and the generation and selection of risk response options. The chapter considers both probabilistic and heuristic methods.

2 Risk Process Selection and Applicability

This chapter discusses and provides examples of the possible differing contexts of NASA activities that reflect the strategic/enterprise, program/project or institutional nature of the associated objectives and domains. The context for these examples is set by examining the flow-down logic of derivation of objectives from the enterprise to the program/project and institutional levels, as per the concepts introduced in Part 1 Chapter 2, for the ultimate purpose of illustrating how RM processes and steps should be selected and applied to fit the type of objective and execution activity being addressed.

From the point of view of an ODRM process execution, the objectives selected, and the associated activities planned and set in motion, constitute in practice an "as-given" context. As such, they are discussed and exemplified here not because their definition and set-up is a part of the execution responsibilities of the organizational entities seeking to implement and apply an ODRM process related to them, but simply to provide realistic exemplification of the operational context that different types of pre-defined agency objectives and activities represent, for the attending ODRM processes are to be selected, adapted, and applied.

2.1 Management of Risk According to Type of Activity Objectives

The NASA RM policy and guidance of NPR 8000.4C defines risk as "risk to the declared objectives of an activity." Since objectives vary substantially in breadth and nature across the NASA domains and the organizational units charged with the execution of the corresponding activities, the nature and depth of the corresponding ODRM process applications needs to be selected and adapted accordingly. In the following, the discussion focuses on examples of different types of objectives and activities that flow down from a primary Enterprise Domain objective.
The primary Enterprise Domain objective considered hereinafter for a flow-down decomposition into "derived objectives" is the NASA long term commitment to a full exploration of the solar system, including its further reaches. From here onward this top-level primary Enterprise Domain objective will be referred to simply as *"Long Term Solar System Exploration."* However, the specifics omitted in this shortened label, i.e.:

a. Exploration of furthest reaches of the solar system,

b. Human-crewed missions, and

c. Establishment of permanent / semi-permanent surface bases,

will continue to be implied, and as such pursued when and where possible, within the scope of this assumed top-level Enterprise Domain objective.

The definition of sub-objectives derived from the assumed primary objective and residing in all three principal domains of NASA activity is the subject of discussion in Section 2.1.1 below.

2.1.1 Example of Multi-domain Objectives Derived from Primary Enterprise Level

Figure 2-1 shows a selective flow-down of sub-objectives that are derived from the *"Long Term Solar System Exploration"* primary objective. The flow-down is called here "selective," because it does not try to provide a full "breadth and depth" exemplification of how the primary objective

might be decomposed, but shows only those portions of the possible decomposition that illustrate how the primary definition can in practice lead to the definition of activity sub-objectives that reside in all three principal NASA activity domains, i.e., Enterprise, Program/Project, and Institutional.

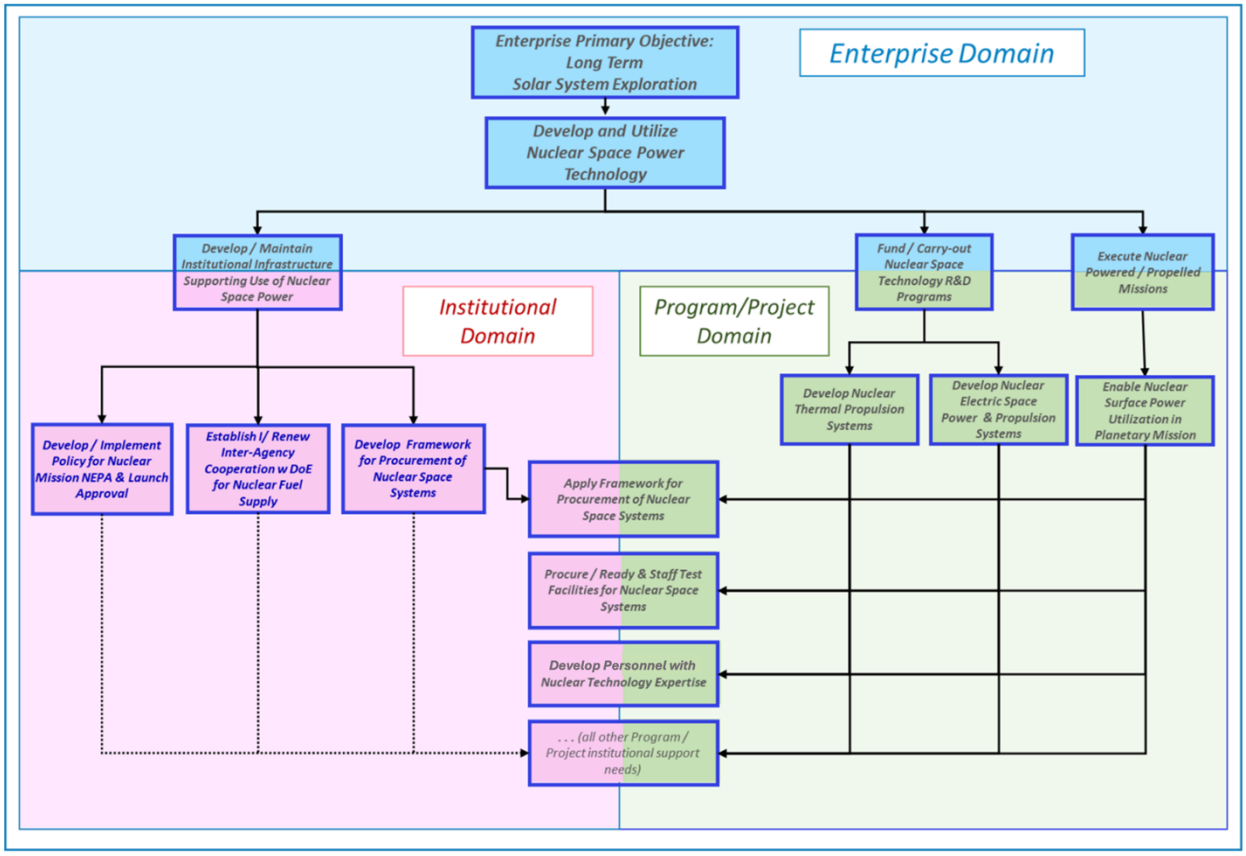


Figure 2-1. Multi-Domain Objectives Derived from the Long-Term Solar System Exploration Primary Enterprise Objective

The sub-objectives illustrated by the figure are color-coded according to the same scheme used earlier in Part 1 Chapter 2 Figure 2-2, i.e., blue indicates objectives and/or activities primarily associated with the Enterprise Domain, pink those primarily associated with the Institutional Domain, and green those primarily associated with the Program/Project Domain. Objectives at the interface between two domains, i.e., formulated in one domain and passed for execution to another domain are colored half-each with the colors of the interfacing domains. Thus, the figure illustrates that the top-level Enterprise Domain objective *"Long Term Solar System Exploration"* and its derived sub-objective *"Develop and Utilize Nuclear Space Power Technology"* is in this example assumed to lead to three sub-objectives:

A. *"Develop/Maintain Institution Infrastructure Supporting Use of Nuclear Space Power,"* which is transferred for further development and execution into the Institutional Domain

B. *"Fund / Carry-out Nuclear Space Technology Research and Development (R&D) Programs,"* which is transferred for further development and execution into the R&D area of the Program/Project Domain

C. *"Execute Nuclear Powered/Propelled Missions,"* which is transferred for further development and execution into the mission portfolio area of the Program/Project Domain.

The principal observations pertaining to the above are as follows:

- Institutional Objective A is "institutional" at the broadest level, i.e., it is directly derived from an agency-level need, rather than from a specific program or project support need. This is unlike other types of institutional objectives of which examples will be given in the following.
- Program/Project Objectives B and C differ in nature, reflecting the maturity of the nuclear technology with which they are concerned, i.e., Objective B reflects the need to carry out technical work in the form of R&D projects for bringing new nuclear space power and/or propulsion technology to a level of readiness and reliability suitable for actual use in operational missions, whereas Objective C concerns the demonstration and operational use of the nuclear technology developed under Objective B, or which may be pre-existing the execution of the latter at a given point in time.
- Examples of the lower level Institutional and Program/Project Domain sub-objectives derived from the above are discussed below in Sections 2.1.1.1 and 2.1.1.2, respectively.

2.1.1.1 Examples of Program/Project Objectives Derived from Enterprise Level Flow-down

Examples of Program/Project Domain objectives produced by the original top-level "Long Term Solar System Exploration" Enterprise Domain objective are included in Figure 2-1 and discussed herein first, before the examples of Institutional Domain objectives also shown by the flow-down illustration in the figure. This is because the Program/Project Domain side of the objectives flow-down produces, besides specific program and project objectives, also program-related and project-related institutional objectives, which are ultimately transferred for execution to the Institutional Domain. These are added therein to the agency-wide institutional objectives that proceed directly from the Enterprise Domain Level. Thus, the institutional objective subject is discussed below in Section 2.1.1.2 with the benefit of having already identified and partially discussed the institutional objectives that are derived from the support needs of any specific individual projects.

Figure 2-1 illustrates the flow-down relationship between Objectives B and C and their respective sub-objectives. Objective B ("Fund / Carry-out Nuclear Space Technology R&D Programs") is assumed to result into the following sub-objectives:

B-1 *"Develop Nuclear Thermal Propulsion Systems"*

B-2 "*Develop Nuclear Electric Power & Propulsion Systems"*

The key observation relative to the above Program/Project Domain objectives is that they are defined in terms specific enough that the corresponding execution may be assumed to take the form of two corresponding technology development projects, e.g., one focused on the development of a viable nuclear thermal propulsion engine for a launch-vehicle upper-stage system, the other on the development of nuclear space reactor systems suitable for providing power to a planet/moon

surface base, or to the electronic components of a spacecraft and the ion-thrusters of its propulsion system.

The example offered in Figure 2-1 of a further flow-down of Objective C (*"Execute Nuclear Powered/Propelled Missions")* consists of the following sub-objective and corresponding mission project definition:

C-1 *"Enable Nuclear Surface Power Utilization in a Planetary Mission"*

The key observation relative to this latter Program/Project Domain objective is that, unlike the R&D oriented Objectives B-1 and B-2 examined above, it defines for its execution an actual operational flight mission, the key objective and execution element of which is the demonstration of feasibility of the design, production, and delivery of a nuclear space reactor for planetary surface utilization.

As discussed in the following section, the B-1, B-2, and C-1 objectives and corresponding projects can be assumed to generate directly related sub-objectives, which are directed at satisfying the project procurement infrastructure needs, test and support-equipment facility needs, and personnel needs for the execution phases. These sub-objectives can be assumed, in a normal execution process, to be transferred for their fulfillment to the Institutional Domain, and as such are identified in Figure 2-1 as examples of "domain interface objectives." For the sake of simplifying the figure illustration, objectives of a similar nature that correspond to the same type of needs from different projects are represented in Figure 2-1 as a single box, rather than being identified with separate boxes to reflect their origination from different projects. This is merely a practical solution to keep the graphical representation of Figure 2-1 as compact and simple as possible. Of course, in real cases the same type of need and objective would, in its formulation and means of fulfillment, take different forms for different projects. Accordingly, in the full list that follows below, the Program/Project Domain to Institutional Domain interface objectives identified in Figure 2-1 are separated out by originating project, with distinct identifying labels and definitions.

The list is as follows:

B-1.1 "*Apply Framework for Procurement of Nuclear Space Systems – for Project B-1"*

B-1.2 *"Procure/Ready & Staff Test Facilities for Nuclear Space Systems – for Project B-1"*

B-1.3 *"Develop Personnel with Nuclear Technology Expertise – for Project B-1"*

B-2.1 *"Apply Framework for Procurement of Nuclear Space Systems – for Project B-2"*

B-2.2 *"Procure/Ready & Staff Test Facilities for Nuclear Space Systems – for Project B-2"*

B-2.3 *"Develop Personnel with Nuclear Technology Expertise – for Project B-2"*

C-1.1 *"Apply Framework for Procurement of Nuclear Space Systems – for Project C-1"*

C-1.2 *"Procure/Ready & Staff Test Facilities for Nuclear Space Systems – for Project C-1"*

C-1.3 *"Develop Personnel with Nuclear Technology Expertise – for Project C-1"*

2.1.1.2 Examples of Institutional Objectives Derived from Enterprise Level Flow-down

The examples of Institutional Domain objectives produced by the original top-level "Long Term Solar System Exploration" Enterprise Domain objective and included in Figure 2-1 are of two different kinds, reflecting what may be considered a more general differentiation between two separate types of institutional objectives, i.e.:

a. Institutional objectives derived from agency-wide higher-level objectives and needs identified within the Enterprise Domain;

b. Institutional objectives derived from the execution level needs of specific programs and projects.

The examples of institutional objectives belonging to the first of the above two classes are:

A-1 *"Develop / Implement Policy for Nuclear Mission National Environmental Policy Act (NEPA) & Launch Approval"*

A-2 *"Establish/Renew Inter-Agency Cooperation with Dept. of Energy for Fuel Supply"*

A-3 "*Develop Framework for Procurement of Nuclear Space Systems"*

The examples of institutional objectives belonging to the second class and associated with project needs defined within the Program/Project Domain have been identified earlier, at the end of Section 2.1.1.1 (see section items B-1.1 through C-1.3).

It is noted that Figure 2-1 indicates with a connection arrow the existence of self-evident relationships between the cross-agency Institutional Domain Objective A-3 *("Develop Framework for Procurement of Nuclear Space Systems"*) and the "interface" Institutional – Program/Project Domain Objectives B-1.1, B-2.1 and C-1.1 *("Apply Framework for Procurement of Nuclear Space Systems – for each of the corresponding projects"*). The assumption reflected in this connection is that any intent to apply commercial practices to the procurement of nuclear space systems would be realized by first developing a generally applicable approach and process, which would be vetted and approved at the overall agency level for any type of specific use; once developed and established, such an approach and process would then be applied to specific project instances and procurement needs.

2.2 Allocation of Objectives for Execution by Organizational and Functional Units

Activity objectives are developed and defined in increasing level of detail as they are flowed down from the top Enterprise Domain formulation level to the Institutional Domain and Program/Project Domain execution level. At the lowest level of detail and decomposition they define actual activities and projects, to be executed, depending on their nature, in either of these two execution domains.

The nature of the activities to be executed also determines their allocation, and the realization of the corresponding objectives, to either organizational units specifically organized as a program or project within one of the technically oriented NASA Mission Directorates, or to mission support and center offices coordinated under the Mission Support Directorate. In either case, the actual fulfillment of staffing, technology and infrastructure needs for activity execution is provided by the resources available at the NASA Centers and Facilities, complemented with any corresponding

resources that NASA deems to bring to bear from commercial contractors, via an appropriate procurement mechanism and process.

Looking once more at the objectives and activities depicted in Figure 2-1, Objectives B-1, B-2, and C-1 are execution level objectives for which it can be assumed that corresponding projects would be defined, set-up, and executed. The provision of human and material resources for the projects, partially represented in Figure 2-1 by the inter-domain sub-objectives B-1.1 thru C-1.3, can correspondingly be assumed to be assigned, for the hosting and staffing needs of each project (Sub-objectives B-1.2, B-1.3, B-2.2, B-2.3, C-1.2, C-1.3), to one of the NASA centers as a primary agent, which may be also supported with personnel, administrative provisions, and/or equipment from other centers and, if necessary, by headquarter mission support offices, on an as-needed basis.

On the other hand, sub-objectives of a more general nature that correspond to cross-agency and/or cross-program needs, such as A-1, A-2, and A-3, can be assumed to become for overall coordination and efficiency of execution, the responsibility of a central agency entity, such as the Mission Support Directorate. However, a considerable if not total share of execution responsibility for the corresponding institutional development and support activities and tasks may be assigned to center-located mission support offices and units.

Once more, it is emphasized that the present discussion is intended to simply reflect, at a conceptual level, the flow and assignment of responsibility across the NASA organization, as presently understood in general terms by the authors of this handbook. This is done for the purpose of illustrating how risk management responsibilities, which are by definition associated with program, project, and institutional activity objectives and corresponding executions, will generally reside with the entities to which the material execution of projects and activities is assigned and entrusted. This will remain generally true, even if the actual flow of objective and activity assignments were in the future to be modified to reflect a different organizational structure and no longer correspond to the conceptual framework represented and discussed here.

2.3 Risk Management Set-up in Program/Project and Institutional Domain Activities

The objective of this section is to illustrate how the nature of a risk management process set-up and execution may differ, depending on the nature of the project and/or activity to which the risk management process is to be applied. For this purpose, the following subsections use as examples the execution-level projects and activities directly corresponding to the objectives discussed as examples in Section 2.1.

The basic general criteria used for the identification of the type of risk management process that is applicable, in a given context and for a given type of project or activity, have been identified in earlier discussions both in Part 1 and Part 2 of this handbook, and can be summarized as follows:

- RIDM risk management processes are applicable in the following two principal types of situations:

    a. At the set-up of a project or activity, when a risk-informed AoA (Analysis of Alternatives) is useful to help decision makers select optimal mission and system architecture and design solutions, among those that appear in theory possible and

feasible – "optimal" in this context indicating a solution that balances benefits and risk in a way that the RIDM AoA indicates to be most reasonable and advantageous;

b. During the execution of a project or activity, when a risk containment and control action involves possible alternative interventions on the mission and/or system design that are of significant overall project impact and complexity, so that a RIDM AoA may be necessary to select the one intervention that appears to be optimal from a risk and cost vs. benefit point of view.

- The CRM process is applicable when project and activity tasks have been defined and are underway, and associated risks can correspondently be identified and need to be evaluated and dealt with.

It is noted that the above criteria are applicable regardless of whether the application of RIDM or CRM processes can be supported quantitatively, or not. As will be illustrated via the examples provided in Chapters 3 and 4 of this Part 2, the applicability of RIDM or CRM processes is in fact independent of whether the execution of the corresponding processes can be quantitatively based, or whether it remains limited to qualitative or semi-quantitative considerations. Quantification of analytical RIDM or CRM processes produces beneficial insights into the risk vs. benefit balances achievable in a project or activity execution. However, risk quantification is contingent upon the availability of information and data which in turn depends on the stage of evolution and maturity of the target projects or activities. Nevertheless, even when such info or data is not readily available or obtainable, very valuable insight and decision support input can still be obtained from a structured, albeit qualitatively based, application of the processes.

2.3.1 Examples of Risk Management Process Selection and Set-up for Program/Project Domain Activities

This section considers one of the examples of Program/Project Domain objectives discussed in Section 2.1, and a correspondingly defined hypothetical project, to identify the risk management processes that may be applicable and can be applied in such a context. The objective considered for this exemplification is Objective C-1 ("*Enable Nuclear Surface Power Utilization in a Planetary Mission"*) and the associated hypothetical project is the set-up and execution of a mission that, from here onward, is referred to as the *"Nuclear Planetary Surface Power Delivery Mission,"* or, in short, the *"NPSPD Mission."* The subsections below briefly discuss the type of risk management processes that are applicable to this example mission at various stages of its initiation and execution.

2.3.1.1 Activity-Planning RIDM for NPSPD Mission Onset AoA

The set-up of a complex planetary mission, as an NPSPD Mission would certainly be, involves a multitude of critical mission and system top-level design choices in which potential advantages and risks need to be carefully considered and balanced against one another. The "Activity Start RIDM" steps and analytical processes discussed in Part 1 Chapter 4 are the ones applicable for this stage of mission initial design and project set-up / initiation.

Key mission and system design choices and factors that would be subject to a RIDM AoA evaluation and decision support process are listed below. They are provided as an example of what may be considered as being within scope, without any claim of completeness or exhaustiveness of the factors listed. In fact, only a formal multi-expert session of key design factors identification, to be executed as part of the RIDM process set-up itself, may provide any assurance of approaching completeness in identification of all the factors that play a significant role in the risk-benefit balance of a mission and system design as complex as that of the NPSPD Mission can be assumed to be.

RIDM-relevant factors of potential interest are listed under the two functional categories of "Mission Design" and "Nuclear System Design," and under an additional category "General Evaluation Factors," which includes the most general performance and risk dimensions that apply to the overall evaluation of any mission or system. Only a subset of these factors will be considered as elements of the RIDM risk trade space to be discussed in the further elaboration of the example. This is done in order to keep the discussion at a level of breadth that makes it more easily explained and understood. However, before that reduction of discussion scope, the factors are first listed below in their more expanded range, including for each of them sub-bullets that help highlight some of the associated pros and cons:

A. Mission Design
    - Single vs. multi-launch mission
        - Target planet / moon
        - Medium vs. heavy launch vehicle
        - Reactor modules delivered in assembled vs. "to-be-assembled" state to planet / moon

B. Nuclear System Design
    - Reactor power level
        - Electric power predicted to be made available
        - Heat transfer / removal system design
        - Power conversion system solution
    - Type of nuclear reactor and fuel
        - Fast / highly-enriched-fuel vs. thermal / lower-enrichment-fuel
        - Launch mass
        - Non-proliferation policy implications
    - System design life

C. General Evaluation Factors
    - Safety
    - Security

- Reliability
- Project and mission execution time and cost

2.3.1.2 CRM for NPSPD Mission Project Execution Risk Management

Once a project initiation RIDM AoA has been completed, leading to the selection of a top-level mission and system design architecture, the overall project objective (i.e., C-1 *"Enable Nuclear Surface Power Utilization in a Planetary Mission"*) is articulated further in a more specific and detailed set of mission and system design objectives, the realization of which will be contingent upon the proper management of any identifiable corresponding risks. Since such an ODRM activity is in this context to address project execution risks, it will normally be based on the application of CRM processes.

Chapter 4 presents a hypothetical breakdown of the NPSPD Mission Project C-1 Objective into a set of mission and institutional objectives applicable specifically to the CRM application examples presented in the rest of the chapter. Based on that definition of project task objectives, the following discussion proceeds to present examples of CRM and Activity-Execution RIDM application, which are intended to illustrate the processes of identification, analysis, and handling of the associated project execution risks.

2.3.1.3 Activity-Execution RIDM for NPSPD Mission Project Execution Risk Management

As established and discussed in Part 1 Chapters 2, 4, and 5, Activity-Execution RIDM is a form of reduced scope RIDM AoA, which is specifically invoked when the selection of an important risk control solution requires careful cost-benefit and risk reduction worth considerations not easily resolved via informal judgment on the part of the decision maker. A special case of this type of RIDM application, called Activity-Rebaselining RIDM, has also been introduced in the same Part 1 chapters. This type of RIDM is applied in the extreme, and hopefully infrequent cases, when a major project risk cannot be controlled without a modification of basic mission or system requirements and design choices – hence the necessity to execute what may be considered an "activity reset" risk-informed AoA to identify an updated mission and /or system top-level baseline architecture and design.

Chapter 4 presents examples of CRM-triggered conditions under which it may be deemed appropriate to invoke the application of Activity-Execution RIDM. In general, it is appropriate to examine alternative ways and paths to achieve risk reduction and control of significant individual risk scenarios identified with CRM processes, and to give due consideration to the pros and cons of such alternative solutions (e.g., their risk reduction worth vs. time and cost of implementation, and possibly the introduction of new significant project risks). In such contexts, Activity-execution RIDM is recommended for application in that subset of cases where the risk being considered is particularly serious and complex, so that the alternative means of controls need to correspondingly be analyzed and understood in sufficient depth and with the support of all the evaluation data that can be brought to bear in the selection decision.

2.3.2 Examples of Risk Management Process Selection and Set-up for Institutional Domain Activities

This section considers one of the examples of Institutional Domain objectives discussed in Section 2.1, and a correspondingly defined hypothetical institutional activity, to identify the risk management processes that may be applicable and can be applied in such a context. The objective considered for this exemplification is Objective A-3 ("*Develop Framework for Procurement of Nuclear Space Systems")* and the associated hypothetical activity is the set-up and execution of an institutional task that from here onward is referred to as the "*Nuclear Space System Procurement Framework Definition*," or, in short, the "*NSSPFD Task.*" The subsections that follow briefly discuss the type of risk management processes that are applicable to this example institutional task at various stages of initiation and execution. Some of the examples discussed in the remaining sections of this chapter will be re-examined and discussed in more detail in Chapters 3 and 4, together with examples directly postulated and formulated in those following chapters.

2.3.2.1 Activity-Planning RIDM for NSSPFD Task Onset AoA

The set-up of an institutional task may have far-reaching outcomes and implications, as would certainly be the case for the selection of a preferred procurement model for a potentially long term and financially significant series of nuclear space power projects and missions. Thus, there is little doubt that the decision process leading up to such a selection would benefit from a careful consideration of the potential advantages and risk of the alternative modes of procurement that can be candidates for adoption.

An Activity-Planning RIDM AoA is the RM tool of choice in such a context, even though the RIDM analytical processes that can be applied in this particular type of RIDM AoA are likely to be for the most part qualitatively, rather than quantitatively, informed. This is because both the advantage/opportunity and risk factors to be considered in this type of institutional task AoA are themselves "soft factors" that do not always lend themselves to a meaningful quantification.

As in the case of the more technically oriented RIDM processes for mission project AoAs, it is useful to apply a structured evaluation process by which the factors to be considered are grouped into a few relevant categories. As in the case of the example of application of the Activity-Planning RIDM processes to a mission project initiation discussed in Section 2.3.1.1, an example set of factor categories, factors, and subfactors to be considered in the RIDM AoA is provided here, with the caveat that this is done without claim of completeness:

A. Procurement Model

- Cost-plus fully Government managed and controlled
  - Priority for performance and safety requirements
- Hybrid (Fixed-price / Cost-plus) Government-Commercial partnership
  - Government retains control of nuclear safety and nuclear system performance requirements in cost-plus portion of procurement
  - Commercial procurement at fixed-price is applied to non-nuclear portion of mission and system procurement

- Full turn-key commercial procurement
  - Commercial contractor fully responsible for system design and operation

B. Nuclear Safety and Launch Approval

- Government control and responsibility for System Safety Analysis (SSA)
  - Application of same high-quality standard process of safety risk assessment
- Contractor responsibility for system SSA, with formal Government review and approval
  - Partial enforcement of quality standards in contractors' safety risk assessment processes
- Full contractor responsibility for SSA
  - SSA validation via independent review – e.g., as per Interagency Nuclear Safety Review Board (INSRB)

C. General Evaluation Factors

- Industrial basis
- Cost advantages
- Schedule advantages
- Satisfaction of political priorities
- Administrative flexibility

2.3.2.2 CRM for NSSPFD Task Execution Risk Management

As in the case of project activities, CRM processes are executed in institutional activities for the management of risks that emerge during execution of a selected and defined set of activities.

As an example, let us assume that the institutional NSSPFD Task has selected a "Hybrid Procurement Model" (HPM) as the contractual framework under which all future nuclear-powered missions shall be procured. The definition of such a framework via the task activities will likely have to address several risks directly consequent and associated with such a course of administrative framework development, such as:

- Schedule and cost impact of coordination of fixed-cost commercial procurement of non-nuclear-safety related part of the system with Government-controlled cost-plus procurement of nuclear-safety-related part of the system;
- Schedule and cost impact of coordination of inter-agency NASA-DoE activities concerning procurement of nuclear fuel;
- Possible safety relevant implications of design characteristics of commercially procured portions of the system classified as non-nuclear-safety related.

These, and any other execution-phase risks for the NSSPFD Task, will have to be properly identified, analyzed / understood, and if necessary countered, within a CRM process set-up for the Task.

2.3.2.3 Activity-Execution RIDM for NSSPFD Task Risk Control AoAs

As for mission projects, Activity-Execution (and in more infrequent cases, Activity-Rebaselining RIDM) may be triggered by CRM during the execution of an Institutional Domain task, in the face of a risk-control decision with potentially significant implications for the entire task or activity.

An example of risk-control question that may call for the execution of an Activity-Execution RIDM would be the in relation to the discovery of a previously unanticipated nuclear-safety implication of a commercially procured system component, which had initially been declared as "non-nuclear-safety-related." The risk-control alternatives to be considered for such a case, and for which an Activity-Execution RIDM may be invoked, might in such a case be:

A. Leave the procurement of the component in the commercial portion and negotiate with the commercial provider the establishment of a special pre-acceptance joint Government-Contractor safety review board to address and resolve the identified safety risk(s); or

B. Transfer the procurement control for the component into the Government side of the HPM and address the risk via application of NASA standards and practices.

Remaining on the same type of example, an Activity-Rebaselining RIDM may be called upon in an extreme case whereby the occurrence of discovery of nuclear-safety-related implications of parts of the system previously classified as "non-nuclear-safety-related" would be become so frequent and pervasive as to call perhaps for a reclassification review of the entire system, or even for the application of a fully Government-controlled [cost-plus] procurement framework model.

3 Example of Activity-Planning RIDM Execution

This chapter provides and discusses an example of the application of the RIDM steps and risk-informed analysis-of-alternatives (AoAs) that are executed at the stage of selecting the conceptual design and architecture of missions, projects, or, more generally, "activities" that are intended to be executed for the realization of explicitly declared objectives.

The discussion presented in Part 1 Chapter 2 and further developed with examples in Chapter 2 of this Part 2 has introduced and illustrated the fundamental principle that informs the NASA RM processes, i.e., that RM in the NASA context is intended to address risk, in its individual specific manifestations, but also at the overall aggregate level, that may affect the realization of objectives set in the three principal domains of NASA activity, i.e., the Enterprise, Program/Project, and Institutional Domains. To emphasize the fact that an unambiguous definition and understanding of organizational objectives and of the relationship between risks and such objectives is to be considered a fundamental pre-requisite for an effective execution of RM processes, this handbook refers to the latter as Objectives-Driven Risk Management (ODRM).

The introductory material of Part 1 Chapter 2 and the examples of the preceding chapter of this Part 2 provide rationale and perspective for why the risk management execution should clearly identify the flow-down of organizational objectives, from the higher levels of definition down to the level where they become tied to specific activities defined and planned for their practical realization. It is via this identification of objectives, as well as of their stage of development, that the appropriate type and combination or RM processes and techniques can be appropriately chosen and applied to address the associated risks. Thus, although the definition of project and activity objectives is in its own right not part of RM, it is a very important input for it, as it determines the RM type, scope, and focus, as Chapter 2 has been intended to illustrate.

3.1 Activity-Planning RIDM Example

Activity-Planning RIDM (AP-RIDM) has been defined and described in Part 1 as the risk-informed AoA process and attending risk analysis techniques that are intended to make as explicit as possible the risk profiles characterizing the performance risk that may affect the achievement of project and/or activity objectives, so that the profiles of alternative system designs and activity execution plans can be compared, and risk-informed deliberations and decisions can be made concerning a preferred project / activity set-up and course of implementation.

The remainder of the present chapter is dedicated to providing a realistic example of AP-RIDM implementation, using a case-study that concerns the application of AP-RIDM to a Program/Project Domain mission and system design, whose intent and scope are directly derived from, and linked to, the nuclear space power demonstration objectives discussed in Chapter 2, Section 2.3.1.

3.2 AP RIDM AoA for Implementation of Program/Project Domain Objectives

The initial set-up, organization, and execution-planning of a complex technical project and mission involves the thorough and technically sound definition and assessment of the trade space covering the possible choices for system / mission architecture, concept of operations ("ConOps"), and key design features. From an RM point of view, consideration of not merely point-value cost-benefit

indices, but of risk profiles and performance uncertainty should be part of the AoA technical investigation applied to identify "optimal" solutions among the mission and project definition alternatives that appear to be possible.

AP-RIDM represents the process and combination of risk analysis techniques that permits an organization to develop and bring to bear the risk-informed perspective of a technically based and quantitative AoA. The example chosen to illustrate this in the remainder of this section is a hypothetical project being set up to implement the Program/Project Domain objective identified in Chapter 2, Sections 2.1.1.1 and 2.3.1 as:

C-1 *"Enable Nuclear Surface Power Utilization in a Planetary Mission"*

The subsections that make up the remainder of the present section follow, aside from some expedient simplification and consolidation of a minor nature, the steps of RIDM execution that have been defined and discussed in their general meaning and form in Part 1, Chapter 4, i.e.:

A. Identify Stakeholders, Understand Expectations and Project Risk Posture
B. Construct a Mission Objectives Hierarchy
C. Identify Performance Measures for Key Mission Objectives
D. Identify Possible Mission Alternatives
E. Set the Risk-Informed Mission Analysis Framework
F. Execute the Risk Analysis of Expected Mission Performance
G. Define Mission Risk Posture with Recommended Risk Tolerances
H. Compare Risk Profiles, Recommend an Alternative, and Document the Rationale

3.2.1 Identify Stakeholders, Understand Expectations and Project Risk Posture

The example case study assumes that a "Planet X Nuclear Power Base (PXNPB) Program Office," set up by the responsible Mission Directorate, has established as a mission campaign objective the enabling of surface nuclear power utilization, in order to demonstrate reliable and safe power generation for future use by a semi-permanent multi-purpose planet exploration base station. A critically important sub-objective of the campaign is to successfully deliver a power production capable nuclear fission reactor to the surface of Planet X (or to one of the moons of Planet X), and a mission intended for such a purpose is being studied and planned. This mission was previously referred to in Chapter 2 as the Nuclear Planetary Surface Power Delivery (NPSPD) Mission, and in the following we shall also be referring to the associated project as the "NPSPD Project."

Besides the primary sponsoring directorate, the Space Technology Mission Directorate (STMD) supports and is a co-sponsor of the mission, seeking demonstration of its surface space power nuclear prototype reactor technology.

Other mission stakeholders include:

- The Science Mission Directorate (SMD)
- The planetary science community interested in the possibility of utilizing space exploration planetary bases with ample supply of power as being used also as bases for future rover science research missions.

- The NASA Headquarters (HQ) Office of Safety and Mission Assurance, who manages the technical independent review of the safety and launch approval of nuclear mission.
- Environmental groups who are concerned about possible radiological contamination of the planets where nuclear reactor power sources may be based.
- Mission support offices (MSOs) within the Mission Support Directorate, who are interested in maintaining and enhancing infrastructure and workforce capabilities in the areas of specialized expertise related to space exploration missions in general, and missions involving nuclear power supply systems in particular.

Specific expectations include:

- The envisioned ConOps is either for:
  a. A single launch of a Reactor Power Module (RPM) to be landed and activated on Planet X or one of its moons by a Transfer and Landing Module (TLM); or
  b. Launches of multiple submodules of the RPM and of a TLM to a high altitude Earth transfer orbit, where the RPM will be assembled and mated to the TLM before initiation of the transfer and landing part of the mission; or
  c. Launches of multiple submodules of the RPM and of separate smaller TLMs directly to Planet X, where the RPM submodules will be delivered for later robotic or astronaut-assisted assembly, carried out as a separate mission.
- The launch date(s) must be within the next 60 months due to the launch window to Planet X.
- The mission should demonstrate successful delivery of an assembled RPM or easy-to-assemble RPM submodules capable of reliable production of an average electric planetary surface power level of 150 kWe for a multi-year duration of time.
- The cost of the mission should be within a cost cap of $1.2B.
- The mission should satisfy the launch safety requirements of National Security Presidential Memorandum-20 (NSPM-20).
- The probability of radiological contamination of Planet X should be minimized, with a goal of no greater than 1 in 1000 (0.1%).
- The mission should serve as a springboard for expansion within NASA and its contractors of a qualified cadre of personnel with nuclear technology capability and expertise.
- The mission should be executed in cooperation with the Department of Energy.
- The mission should utilize to the extent that may be possible commercial suppliers of power system components.

Particularly important in this RIDM step is to develop a clear understanding of the risk posture that the project decision makers intend to apply in the decision processes affecting the definition and execution of the project and mission. The risk posture, as defined in NPR 8000.4C, is the combination of levels of risk tolerance in the project and mission Performance Measures (PMs) that is considered appropriate by the project decision makers and stakeholders. Thus, risk posture can eventually be defined in quantitative terms by the maximum level of risk that is considered acceptable in each dimension of performance. At early stages of the RIDM process it should be defined and perhaps "negotiated" at least in qualitative terms. For the NPSPD Project, it is assumed

that for the performance dimensions that are considered most important (i.e., the so called "key performance measures' – KPMs) the risk posture is defined in the following terms:

- PMs that refer to technical mission performance and success may be assigned a "medium" value of risk tolerance because of the pioneering and technology-demonstration nature of the mission.
- PMs referring to nuclear safety, and more specifically, public safety should be assigned a "very low" risk tolerance value, because of the severe political fallout that any radiological release would cause, even if it were to be small and largely inconsequential.
- PMs referring to project cost and schedule should both be assigned a "low" risk tolerance: in the case of cost PMs. This is because of the difficulty to secure funding and project continuation in case of any cost overrun; in the case of schedule because, in addition to the cost implications of any delay, the project timeline is strictly conditioned by the launch window within which the Planet X mission must be initiated, in order to be practically possible (or otherwise have to be postponed until the next launch window, which may result in the project being altogether cancelled).
- Finally, PMs related to the application of procurement and staffing institutional policy preferences (e.g., staff development policy, commercial procurement policy) may be assigned a "medium" value of risk tolerance because of the recognized objective difficulty of applying the policy preferences, vis-à-vis the realities of the job market for prospective nuclear experts and of the industrial base available for procurement of certain types of nuclear technology items.

The application of the above risk posture / risk tolerance criteria is further discussed in Section 3.2.7.

3.2.2 Construct a Mission Objectives Hierarchy

From the generic top-level objective of "Project Success," for the preparation and execution of an identified mission, the stakeholder expectations that have been captured are organized via an objectives hierarchy that decomposes the top-level objective through the mission execution domains of "Technical," "Safety & Compliance (including cybersecurity and physical security)," and "Cost, Schedule, & Institutional," producing a set of performance objectives at the leaves. Figure 3-1 and Figure 3-2a, b, c illustrate such a decomposition of mission objectives, which in the case of the NPSPD Project and Mission example is executed in two successive steps (respectively shown in Figure 3-1 and Figure 3-2), down to the level of detail that permits the definition of quantitative PMs associated with each objective decomposed at the lowest level that appears to be appropriate for the purpose.

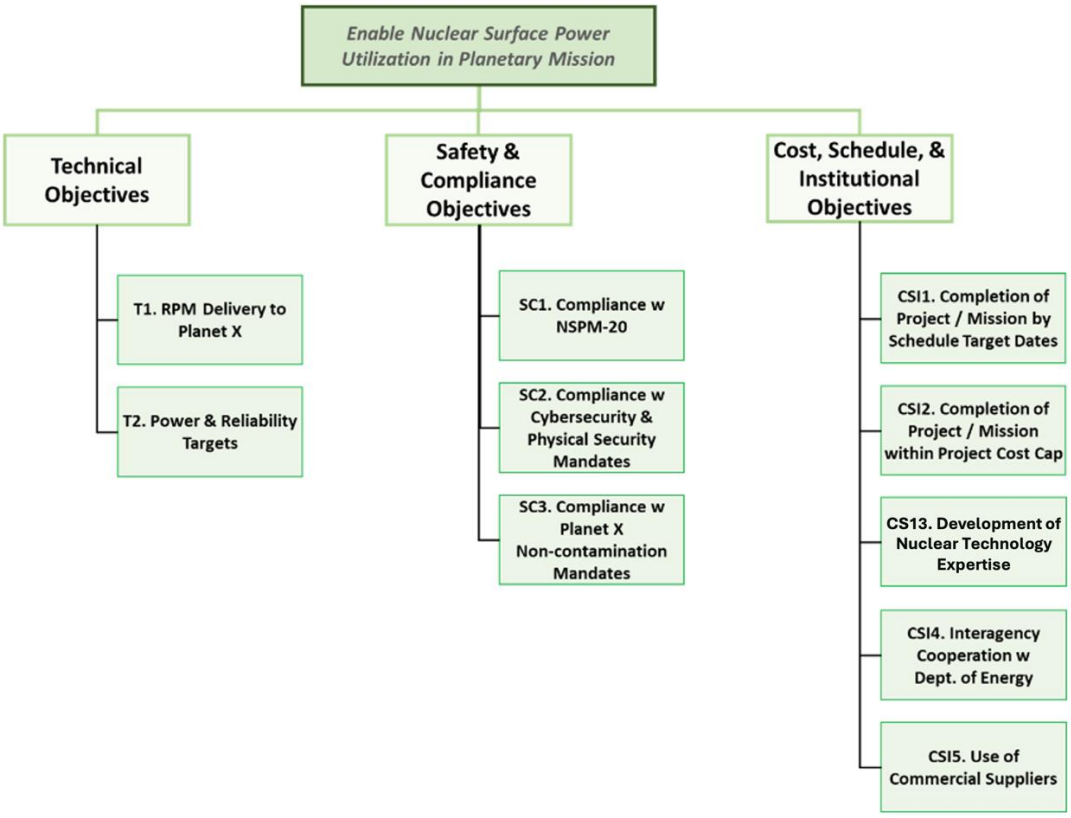


Figure 3-1. Upper Tier of Objectives Hierarchy for the NPSPD Mission Example

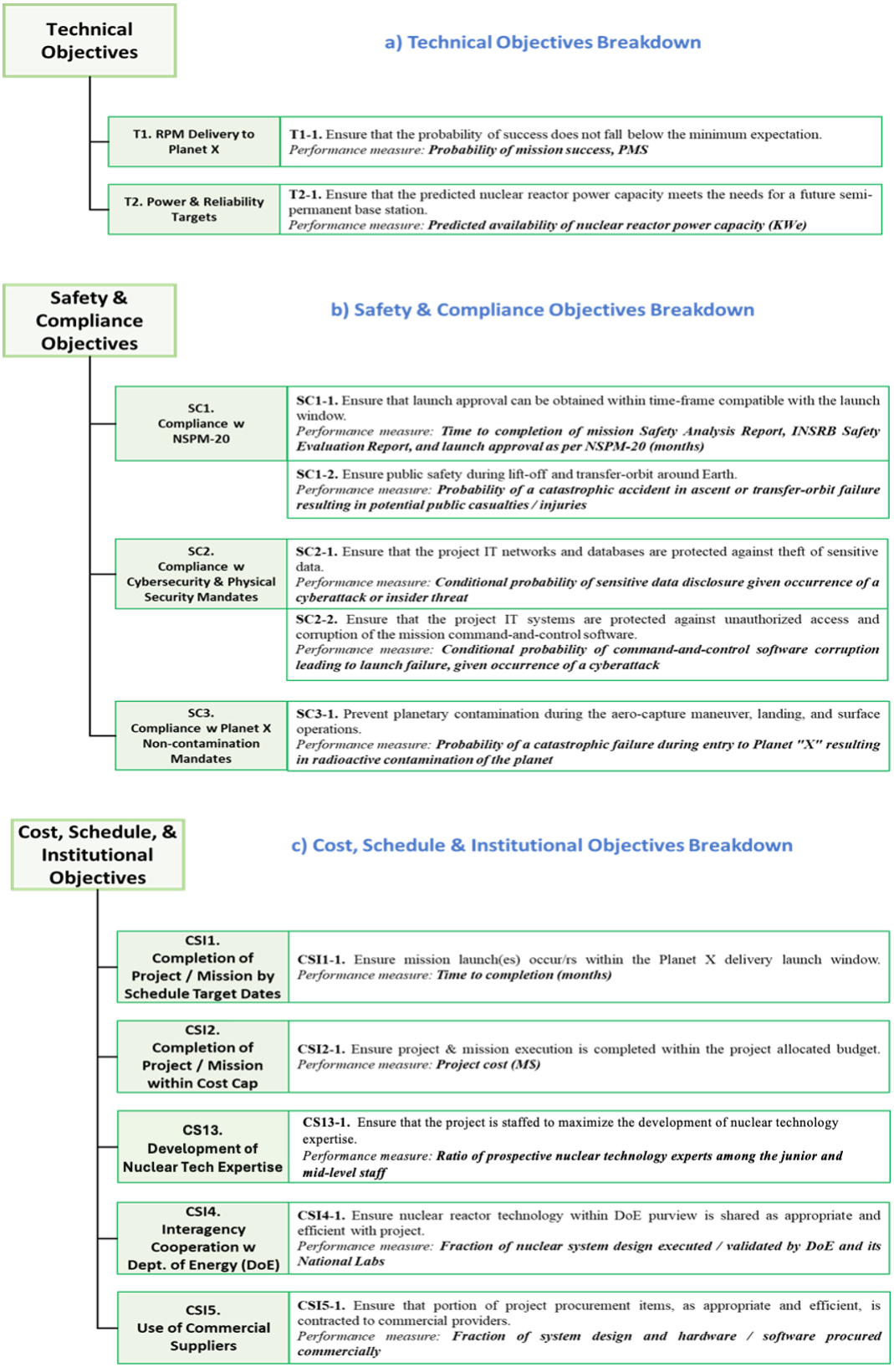


Figure 3-2. Lower Tier of Objectives Hierarchy for the NPSPD Mission Example

3.2.3 Identify Performance Measures for Key Mission Objectives

PMs should be identified and associated with each performance objective, along with any applicable imposed constraints. Whenever applicable and possible such PMs should be objectively defined and quantifiable. This allows the assessor to identify, out of a set of mission architecture and project definition alternatives initially seen as being theoretically possible, one or more alternatives that the RIDM risk-analytical process would indicate as being optimal. "Optimal" in this context means that any such alternative would be shown by the RIDM analysis to keep underperformance risk, across the range of PMs that quantify project objectives, at or below the risk tolerance levels corresponding to the risk posture indicated by project stakeholders and decision makers.

For the NPSPD project/mission example being considered, the full set of objectives and PMs is assumed to be the one implied by the Figure 3-2 illustration, as for reader's convenience summarized below in Table 3-I. The table also lists the imposed constraints that are assumed to be associated with some of the PMs.

Table 3-I. NPSPD Mission Objectives, Performance Measures, and Constraints

Objective Domain	Objective Definition	Performance Measure(s)	Imposed Constraint(s)
Technical	RPM Delivery to Planet X	Probability of Mission Success (PMS)	
	Power & Reliability Targets	Power Availability	
Safety & Compliance	Compliance w NSPM-20	Time to completion of SAR & SER	
		Probability of accidents causing radiological exposure to public	As per NSPM-20 Tier II limits
	Compliance w Cybersecurity & Physical Security Mandates	Conditional probability of sensitive data disclosure	
		Conditional probability of command & control compromise	
	Compliance w Planet X Noncontamination Mandates	Probability of radiological release on Planet X	
Cost, Schedule, & Institutional	Completion by Schedule Target Dates	Time to assembled RPM leaving Earth transfer-orbit	60 months
	Completion within Cost Cap	Total project cost	$1.2B
	Interagency Cooperation w DoE	Percent of budget committed to DoE participation in nuclear system design	
	Use of Commercial Suppliers	Percent of budget committed to commercial procurement	
	Development of Nuclear Technology Expertise	Percent of prospective nuclear experts among junior/mid-level staff	

In practical terms, in order not to have to deal with an overly extended trade space in the analytical portion of the RIDM process, it may be expedient to identify an order of importance and priority for the project objectives and execute the AoA in a staged fashion. This is further discussed and exemplified in Section 4.2.5.

3.2.4 Identify Possible Mission Alternatives

Mission and project execution alternatives that appear to be deserving of consideration can be identified and listed by doing the following:

a) Identify the key mission architecture, system design, and project execution choices that appear to be possible, when considered individually;
b) Structure such choices in a "Trade Tree" that considers and shows the combinations of choices that appear to be logically compatible (e.g., a very heavy RPM would be compatible with a "heavy" launch vehicle single launch, but not with a "medium-light" launch vehicle launch);
c) Further evaluate the Trade Tree in qualitative mode, to eliminate from full analytical consideration those solution alternatives of architecture, design, and/or execution combinations that clearly appear to be either altogether unfeasible or associated with high risk in one or more of the high priority PM dimensions.

3.2.4.1 Possible NPSPD Projects and Mission Choices

Table 3-II below provides an example of key project and mission choices that may be initially considered individually possible. "Individually" in this context means that each system design or mission option listed in the table appears possible when its implementation is envisioned independently of its likely interactions and effects on the other options and solutions being considered. Consideration of the latter factors, first on a qualitative basis, and then from a risk perspective, is part of the RIDM process steps that follow.

Table 3-II. Possible NPSPD Mission / Project Options

RPM Fuel Enrichment	Key Project Execution Options	RPM Assembly & Launch Execution	Launch Vehicle Class
High Enrichment	RPM Provided by Dept. of Energy	Full Assembly and Launch from Earth Launch Site	NASA Heavy Launch Vehicle (NHLV)
< 20% Enrichment	RPM Procured Commercially	Two RPM Submodules Separately Launched, Assembled in Earth Orbit for Delivery to Planet X	Commercial Medium Launch Vehicle (CMLV)
		Two RPM Submodules Separately Launched & Assembled on Planet X	

The contents of the table should at this point be interpreted as indicating that each possible combination of mission design and execution choices identified therein may be theoretically possible. The identification of the combinations of choices that constitute a "feasible alternative" is the subject of discussion in the following section.

The following is assumed and holds, for the example being discussed, with regard to the meaning of the design and execution choices listed in the table:

RPM Fuel Enrichment: This reactor module design choice concerns the degree of enrichment in U_{235} that is selected for the nuclear fission reactor fuel. U_{235} is the fissile isotope of uranium, which is present in small percentage in the mined ore. To make viable fission fuel, the percentage of U_{235} in the total uranium material used as fuel has to be increased. If it is increased above the 20% limit, the fuel is considered to be "highly enriched" and falls under use limitations due to US policy and international treaties regulating the availability of weapon grade fissile material. The level of enrichment, on the other hand, has a strong impact on the design of a nuclear reactor, as only highly enriched fuel can be used to design a "fast reactor" – i.e., a reactor where the neutron flux that sustains the fission reaction is maintained at high neutron energy levels; whereas low enrichment fuel can in practice be used only if the reactor is made to operate as a "thermal reactor," " – i.e., a reactor where the neutrons that sustain the fission reaction are made to lose energy down to the equivalent of ambient temperature by making them collide and bounce off the nuclei of a "moderator" material (a low mass number element like hydrogen, deuterium, helium, etc.). Whether a power reactor that has to travel in space as spacecraft payload is a fast or a thermal reactor may have significant mission design implications, particularly in regard to the whether a heavy lift or medium lift capability launch vehicle may be used, since thermal reactors are generally larger in mass and volume than fast reactors.

RPM Provided by Department of Energy or Commercially: The U.S Department of Energy is the U.S. agency that is generally assigned responsibility for the design of nuclear reactors to be used by the U.S Government, and is also assigned the responsibility of controlling the utilization of nuclear fuel, more in particular to make sure that highly enriched uranium (HEU), i.e. uranium enriched in U_{235} above the 20% limit, is not disseminated beyond the control of the U.S. Government.

RPM Assembly & Launch Execution: This concerns the option of launching the RPM already assembled in one piece, or of designing it as modules that can be assembled in space or at destination on the Planet X surface. The advantages of the latter solutions are that the payload weight is split in a way that permits the use of launch systems of lesser lift capacity, and also, in terms of nuclear safety, that the RPM is divided in submodules that are by definition subcritical, making the event of an accidental nuclear criticality (i.e., the triggering of an unwanted and uncontrolled fission reactor) practically impossible. The drawbacks are in the complexity and difficulty of designing the RPM in a modular way that permits assembly in space or on a remote planet surface, by means of astronaut or robotic operations.

Launch Vehicle Class: This choice concerns the possibility of using, to execute the whole missions or portions thereof, a NASA-provided heavy-lift launch vehicle (NHLV, designed and owned by NASA) or a commercial medium-lift launch vehicle (CMLV) procured via a launch services contract. The selection of one option over the other is determined by the need for more or less payload mass launch capability, which is in large part determined by the RPM design and assembly choices (see above). The use of a CMLV or NHLV, with single or multiple launches as an associated choice, has of course cost and schedule, as well as reliability and safety, implications.

3.2.4.2 Identification of Feasible Alternatives

In the context of the RIDM AoA process, ***an "alternative" is a combination of the specific choices that can be made and implemented, for the key individual system design and project/mission execution options that are theoretically possible***.

In practical terms, by consideration of any clear-cut mutual incompatibilities among some of the associated individual design and/or execution choices, some alternatives may be immediately identified as being either not feasible, or highly uncertain, or otherwise questionable for other obvious reasons. As an example of this, the case was cited above of an RPM design involving a reactor of very high mass/weight that may immediately be judged to be incompatible with the selection of a single mission launch on a medium launch vehicle. To systematically consider and screen out from further analysis, on an initial qualitative basis, all such cases of unfeasible alternatives, it is useful to use as an aid a "Trade Tree" that lays out all the possible combinations of individual options choices that are possible. Table 3-III below shows the trade tree that applies for the alternatives corresponding to the theoretically possible combinations of choices for the individual options identified above in Table 3-II.

Strictly speaking the table presents the mission attribute compatibility evaluation in "trade matrix," rather than "trade tree" form, as the former is more compact visually and can more conveniently include a column documenting in comment form the rationale for keeping or eliminating an alternative. To make clear to readers the equivalence of the tree and matrix formats, the trade tree equivalent to the Table 3-III matrix is also shown, in Figure 3-3 below.

In the current example it is assumed, as a pre-analysis screening criterion, that not only the clearly unfeasible alternatives, but also those that appear to be "not-recommended" because of intrinsic inefficiency or very uncertain feasibility, should be excluded from further consideration. On the basis of this criterion and the qualitative evaluations shown in Table 3-III, the surviving alternatives to be forwarded to the more detailed downstream analytical processes are those listed below in Table 3-IV.

The next step of the example process addresses the set-up of the analytical framework to be used in the objective and quantitative evaluation of the risk levels associated with each potentially viable alternative.

Table 3-III. Trade Matrix of Possible NPSPD Mission / Project Alternatives

RPM Fuel Enrichment	Key Project Execution Options	RPM Assembly & Launch Execution	Launch Vehicle Class (NHLV / CMLV)	1st Order Feasibility (F/UC/NR/UF)	Rationale
			NHLV = Heavy Launch Vehicle CMLV = Medium Launch Vehicle	F = Feasible UC = Uncertain NR = Not Recommended UF = Unfeasible	
High Enrichment	RPM Provided by Dept. of Energy	Full Assembly & Launch from Earth Launch Site	NHLV	F	1 - Procurement via Dept. of Energy may allow NASA to obtain permission to use of highly enriched fuel restricted by nuclear non-proliferation policies. 2 - Launch of fully-assembled RPM is enabled by use of NHLV
High Enrichment	RPM Provided by Dept. of Energy	Full Assembly & Launch from Earth Launch Site	CMLV	UC	1 - Procurement via Dept. of Energy may allow NASA to obtain permission to use of highly enriched fuel restricted by nuclear non-proliferation policies. 2 - Use of CMLV may not provide launch mass capability sufficient for launch of fully-assembled RPM.
High Enrichment	RPM Provided by Dept. of Energy	RPM submodules launched separately and assembled in Earth Transfer Orbit	NHLV	NR	1 - Procurement via Dept. of Energy may allow NASA to obtain permission to use of highly enriched fuel restricted by nuclear non-proliferation policies. 2 - Use of NHLV may not be necessary if RPM submodules are launched separately, and subsequently assembled in orbit.
High Enrichment	RPM Provided by Dept. of Energy	RPM submodules separately launched and delivered to Planet X	NHLV	NR	2 - Procurement via Dept. of Energy may allow NASA to obtain permission to use of highly enriched fuel restricted by nuclear non-proliferation policies. 2 - Use of NHLV may not be necessary if RPM submodules are launched separately, and subsequently assembled in orbit.
High Enrichment	RPM Provided by Dept. of Energy	RPM submodules launched separately and assembled in Earth Transfer Orbit	CMLV	F	1 - Procurement via Dept. of Energy may allow NASA to obtain permission to use of highly enriched fuel restricted by nuclear non-proliferation policies. 2 - Separate launches of RPM submodules permit use of CMLVs.
High Enrichment	RPM Provided by Dept. of Energy	RPM submodules separately launched and delivered to Planet X	CMLV	F	1 - Procurement via Dept. of Energy may allow NASA to obtain permission to use of highly enriched fuel restricted by nuclear non-proliferation policies. 2 - Separate launches of RPM submodules permit use of CMLVs.
High Enrichment	RPM Procured Commercially	n/a	n/a	UF	1 - Commercial procurement of nuclear reactors using highly enriched fuel is not allowed by U.S. policy.
< 20% Enrichment	RPM Provided by Dept. of Energy	Full Assembly & Launch from Earth Launch Site	NHLV	F	1 - RPM using low enrichment fuel will have relatively large volume and mass, and require the use of an NHLV for a single launch of the assembled module.
< 20% Enrichment	RPM Provided by Dept. of Energy	Full Assembly & Launch from Earth Launch Site	CMLV	UF	1 - An CMLV does not have sufficient launch mass capability to launch an RPM using low enrichment fuel, with associated large volume and
< 20% Enrichment	RPM Provided by Dept. of Energy	RPM submodules launched separately and assembled in Earth Transfer Orbit	NHLV	NR	1 - Use of NHLV is not necessary if RPM submodules are launched separately, and subsequently assembled in orbit.
< 20% Enrichment	RPM Provided by Dept. of Energy	RPM submodules separately launched and delivered to Planet X	NHLV	NR	1 - Use of NHLV is not necessary if RPM submodules are launched separately, and subsequently assembled in orbit.
< 20% Enrichment	RPM Provided by Dept. of Energy	RPM submodules launched separately and assembled in Earth Transfer Orbit	CMLV	F	1 - Separate launches of RPM submodules permit use of CMLVs.
< 20% Enrichment	RPM Provided by Dept. of Energy	RPM submodules separately launched and delivered to Planet X	CMLV	F	2 - Separate launches of RPM submodules permit use of CMLVs.
< 20% Enrichment	RPM Procured Commercially	Full Assembly & Launch from Earth Launch Site	NHLV	F	1 - RPM using low enrichment fuel will have relatively large volume and mass, and require the use of an NHLV for a single launch of the assembled module.
< 20% Enrichment	RPM Procured Commercially	Full Assembly & Launch from Earth Launch Site	CMLV	UF	1 - An CMLV does not have sufficient launch mass capability to launch an RPM using low enrichment fuel, with associated large volume and
< 20% Enrichment	RPM Procured Commercially	RPM submodules launched separately and assembled in Earth Transfer Orbit	NHLV	NR	1 - Use of NHLV is not necessary if RPM submodules are launched separately, and subsequently assembled in orbit.
< 20% Enrichment	RPM Procured Commercially	RPM submodules separately launched and delivered to Planet X	NHLV	NR	1 - Use of NHLV is not necessary if RPM submodules are launched separately, and subsequently assembled in orbit.
< 20% Enrichment	RPM Procured Commercially	RPM submodules launched separately and assembled in Earth Transfer Orbit	CMLV	F	1 - Separate launches of RPM submodules permit use of CMLVs.
< 20% Enrichment	RPM Procured Commercially	RPM submodules separately launched and delivered to Planet X	CMLV	F	1 - Separate launches of RPM submodules permit use of CMLVs.

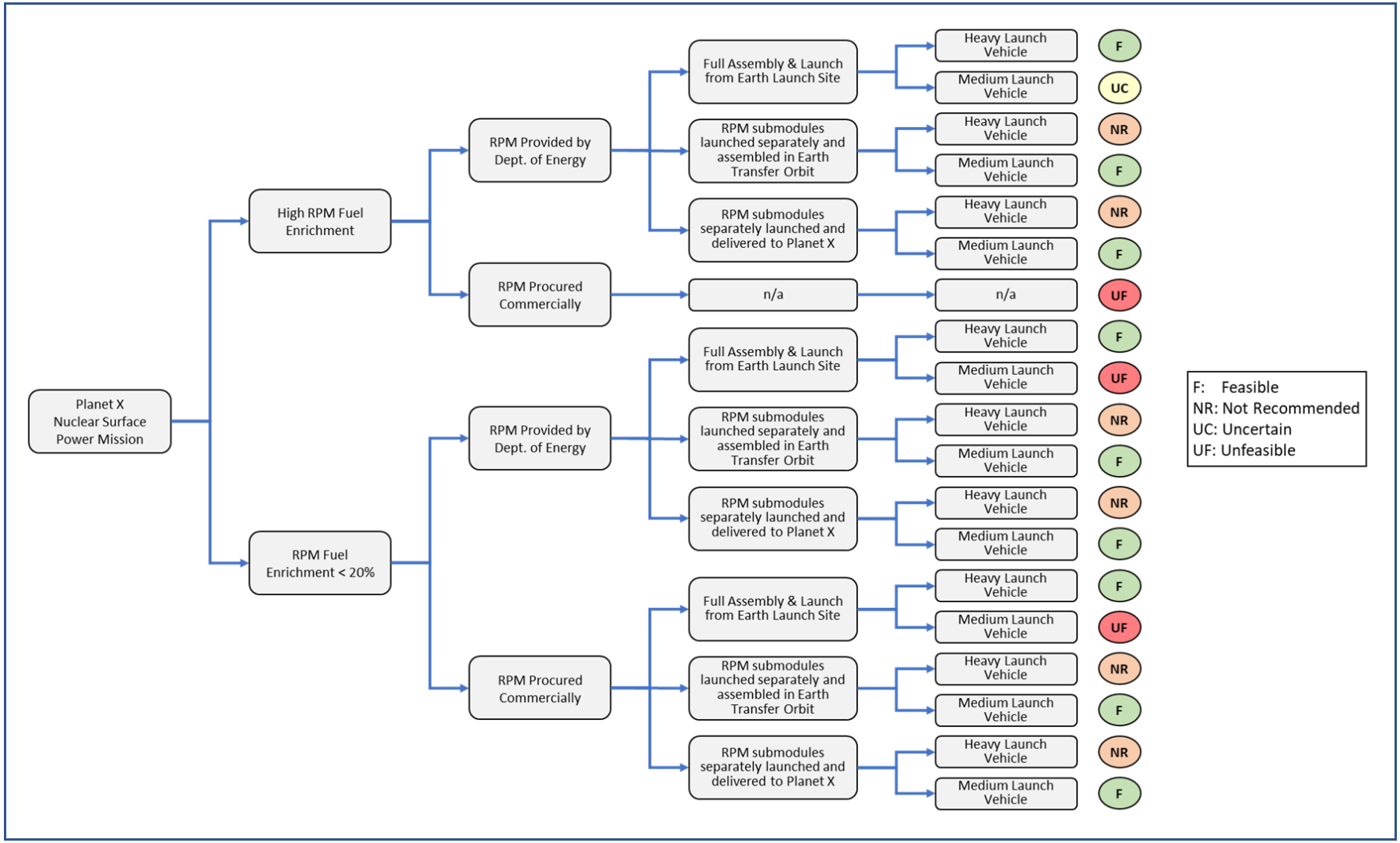


Figure 3-3. Trade Tree of Possible NPSPD Mission / Project Alternatives

Table 3-IV. Feasible Alternatives to Be Forwarded to Risk Analysis

Alternative	RPM Fuel Enrichment	Project Execution	RPM Assembly & Launch Execution	Launch Vehicle
A1	High Enrichment	RPM Provided by Dept. of Energy	Full Assembly & Launch from Earth Launch Site	NHLV
A2	High Enrichment	RPM Provided by Dept. of Energy	RPM submodules launched separately and assembled in Earth Transfer Orbit	CMLV
A3	High Enrichment	RPM Provided by Dept. of Energy	RPM submodules separately launched and delivered to Planet X	CMLV
A4	< 20% Enrichment	RPM Provided by Dept. of Energy	Full Assembly & Launch from Earth Launch Site	NHLV
A5	< 20% Enrichment	RPM Provided by Dept. of Energy	RPM submodules launched separately and assembled in Earth Transfer Orbit	CMLV
A6	< 20% Enrichment	RPM Provided by Dept. of Energy	RPM submodules separately launched and delivered to Planet X	CMLV
A7	< 20% Enrichment	RPM Procured Commercially	Full Assembly & Launch from Earth Launch Site	NHLV
A8	< 20% Enrichment	RPM Procured Commercially	RPM submodules launched separately and assembled in Earth Transfer Orbit	CMLV
A9	< 20% Enrichment	RPM Procured Commercially	RPM submodules separately launched and delivered to Planet X	CMLV

3.2.5 Set the Risk-Informed Mission Analysis Framework

Setting up the risk-analytical framework for the alternatives that need to be comparatively assessed and evaluated is a process that can be described and executed in terms of the practical steps that are discussed in the following.

1. Decide whether it is appropriate to establish an order of priority, or even a smaller subset for analysis, among the PMs by which the alternatives are to be evaluated.

   Explanation / Discussion: Table 3-I identifies a total of twelve PMs by which the alternatives can be evaluated: two for the "Technical Performance" domain, and five each for the "Safety & Compliance" and "Cost, Schedule & Institutional" domains. The RIDM risk-analytical process, if applied to the full range of PMs, would require executing the risk-analysis and risk-informed deliberation and selection of a preferred alternative by taking into account the estimated risk-profiles in each of the twelve performance dimensions identified in Table 3-I. A possible heuristic approach, which will be followed

and illustrated in the current example, is to identify a smaller subset of "key performance measures" (KPMs) by which the alternatives can be evaluated. In a real project context, this reduction of evaluation dimension must obviously be decided on the basis of input from the decision maker(s) responsible for selection or recommendation of the preferred alternative.

2. Identify the factors (in mathematical terms, the "independent variables") that are believed to determine the performance outcome in each of the performance dimensions being quantified by the PMs. In mathematical terms, the PM "dependent variables" will then be expressed and represented as functions of these independent variables via appropriate analytical models.

3. Identify and express via analytical models the functional / logical relationships among the independent variables identified per Step 2 and the PMs, including any significant interdependencies among the PMs.

   Explanation / Discussion: It may be useful to initially use a qualitative representation of the relationships and interdependences among the variables included in the overall analytical risk models. A graphic representation paradigm well suited for this purpose is the one provided by Influence Diagram (ID) / Bayesian Belief Networks (BBNs) [1], even if initially applied in its purely qualitative form of display of causality flow from input to output model variables, and through any additional intermediate variables that may be relevant to understand the nature and extent of the causality relationships. Use of this type of modeling aid is illustrated in the following for the example at hand.

4. Assemble and tie together all the pieces of analytical models expressing the functional / logical relationships between independent and dependent variables (from model "inputs" to "outputs").

The above steps are illustrated below as follows:

Step 1 : For the example being considered, it is assumed that the decision makers and stakeholders have converged on the identification of the following five of the twelve original PMs listed in Table 3-I, as those that are to be treated and evaluated as KPMs:

1. Probability of Mission Success (PMS) – Technical Performance Objective
2. Probability of Radiological Release (PRR) (affecting public) – Safety & Compliance Objective
3. Time to Launch Readiness (TLR) – Cost, Schedule, & Institutional Objective
4. Cost of Project (CP) – Cost, Schedule, & Institutional Objective
5. Expert Staff Development Ratio (ESDR) – Cost, Schedule, & Institutional Objective

Steps 2-4 : The identification of the functional dependencies among input independent variables and the PMs of concern can be carried out in a number of ways, but the use of influence diagrams (IDs) and/or Bayesian belief networks (BBNs) can provide a useful aid for this step. For the purpose of identifying dependencies, IDs or BBNs may just be used in their initial graphical form,

i.e., without full definition of discrete states for all variables that appear in the models, and of the associated conditional probabilities linking the states. In their bare graphical form, thus such models indicate what variables are dependent on which other variables.

For the example considered, Figure 3-4 to Figure 3-6 depict the relationships of concern. More specifically, Figure 3-4 gives the overall relationship map and identifies all the variables of concern, including intermediate variables that need to be considered, in order to better understand the connections between the independent input variables and the KPM outputs. Figure 3-5 and Figure 3-6, on the other hand, separate out the model portions that are independent of one another and individually include only the variables that are indeed connected by direct or indirect cause-effect relationships.

The interpretation of the ID graphic representation is as follows:

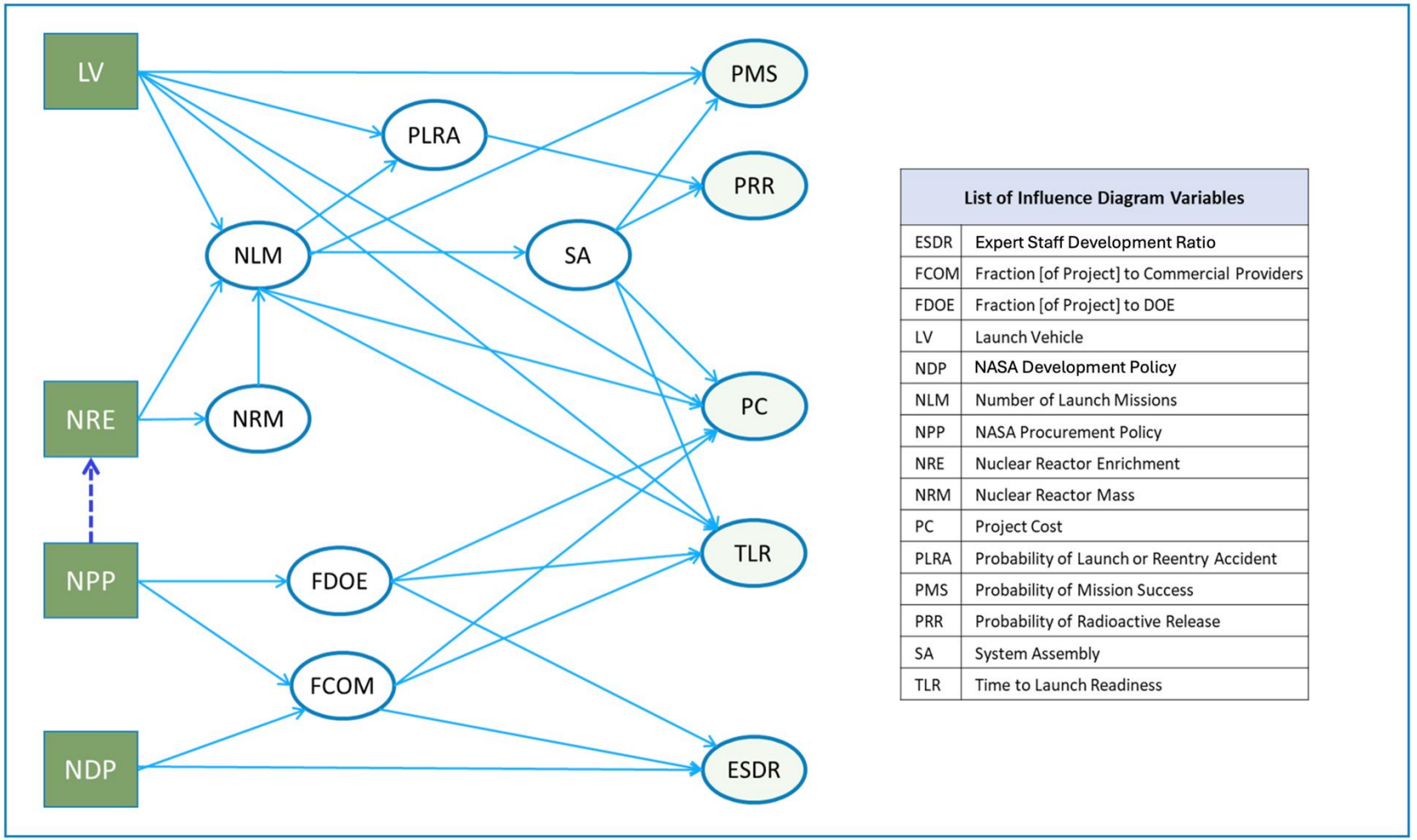
a. Square nodes represent design or mission choices that are under the full control of project and mission managers.
b. Rounded nodes represent mission variables that are either independent inputs governed by external processes or conditions, or are dependent variables within the operational and physical constraints of the mission.
c. Arrowed edges represent cause-effect dependencies among variables.

Thus, for example, the ID graph in Figure 3-5 indicates that the variable PLRA (Probability of Launch or Reentry Accident) depends on the launch vehicle (LV) decision (for the type of launch vehicle selected), and on the variable NLM (Number of Launch Missions). In turn NLM depends itself on the LV decision and on other factors / variables, as shown by the figure. In mathematical terms this would be indicated by the following formulations:

PLRA = f(LV, NLM), where NLM = g(LV, NRM), NRM = h(NRE), NRE = i(NPP)

In the above, f, g, h, I, represent mathematical/logic functions or algorithms, which define a dependent variable in terms of the variable identified in parentheses.

It is noted that in all the ID models shown in Figure 3-4 to Figure 3-6, the variables selected as being the KPMs upon which the AoA selection is to be primarily predicated are identified by the corresponding nodes being shown as filled in pale green color



List of Influence Diagram Variables	
ESDR	Expert Staff Development Ratio
FCOM	Fraction [of Project] to Commercial Providers
FDOE	Fraction [of Project] to DOE
LV	Launch Vehicle
NDP	NASA Development Policy
NLM	Number of Launch Missions
NPP	NASA Procurement Policy
NRE	Nuclear Reactor Enrichment
NRM	Nuclear Reactor Mass
PC	Project Cost
PLRA	Probability of Launch or Reentry Accident
PMS	Probability of Mission Success
PRR	Probability of Radioactive Release
SA	System Assembly
TLR	Time to Launch Readiness

Figure 3-4. Overall Influence Diagram Identification of Mission Variable Cause-Effect Relationships

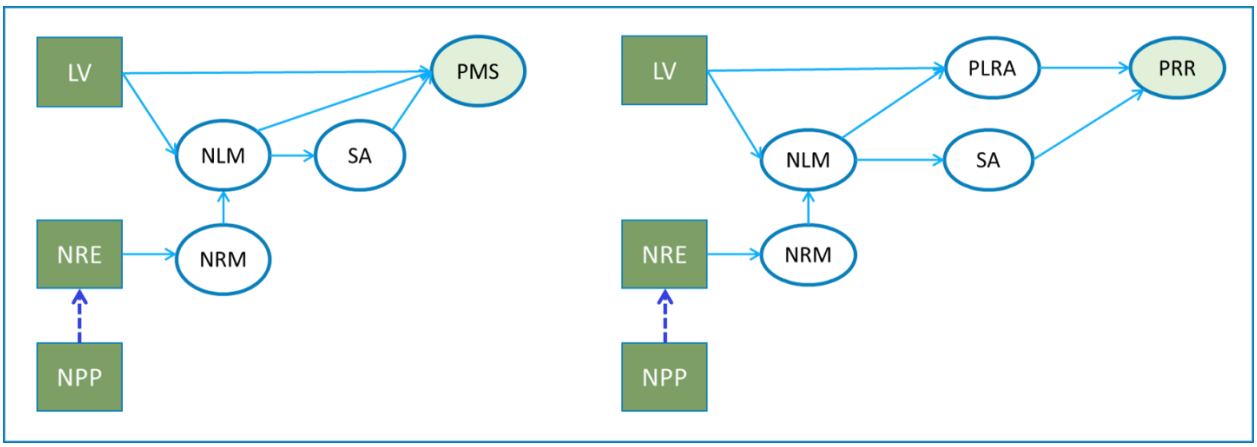


Figure 3-5. Cause-Effect Relationships for Technical Performance and Safety & Compliance Variables

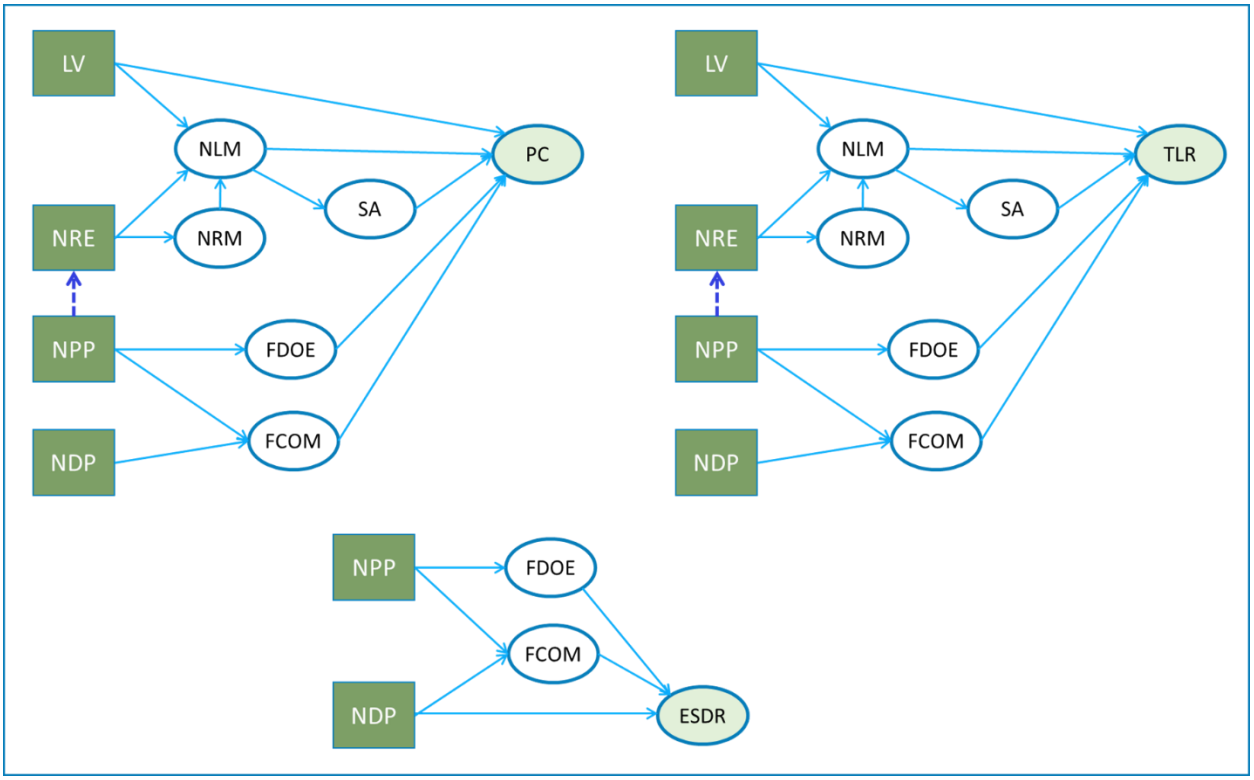


Figure 3-6. Cause-Effect Relationships for Cost, Schedule, & Institutional Variables

3.2.6 Execute the Risk Analysis of Expected Mission Performance

Once variable functional dependencies are identified and formulated, the actual probability distributions of the KPM variables can be derived by execution of the following steps:

1. Use historical data and/or engineering judgment and/or sub-analyses to estimate

uncertainty and variability in all the independent model-input variables and represent such uncertainty / variability via appropriately chosen probability distributions.

2. Derive performance-measure probability distributions via Monte Carlo simulations carried out via the model(s) assembled per Step 3 of Part 1 Section 4.7.3, sampling from the input variable distributions estimated per Step 1 above.

It is noted that, in those cases where an exact deterministic formulation of terms like the f, g, etc. mentioned above cannot be identified, the ID and/or BBN paradigm offers the alternative of defining the corresponding variable-to-variable relationships in the form of variable discrete states and associated joint conditional probability distributions [1]. I.e., the probability of a variable to be in a specific state (e.g., each of a set of discrete values by which each variable is approximately represented) is expressed as a conditional probability of that variable state, given that the set of variables that are identified as direct inputs to the variable are in certain specific combination of their respective states. This allows one to obtain, instead of full continuous probability distributions of the PMs over their defined ranges, obtained via mathematical or algorithmic definitions quantified via Monte Carlo techniques, discrete approximations thereof, obtained via quantification of the ID and/or BBN models formulated for the variables of concern. For more details on this method of carrying out the PM risk quantification, please refer to the extensive public domain literature covering the subject of BBN and ID modeling and quantification.

For the purpose of the example being discussed here, it is assumed that KPM continuous probability distributions could be derived. In order not to make the example illustrations too extensive and complicated, the corresponding results are shown and discussed only for the subset of alternatives identified in Table 3-IV as #7, #8, and #9. In practical terms, this would be the sub-set of mission design and execution alternatives to choose from if the following criteria were indicated by decision makers as must-follow decision priorities:

A. The mission should avoid the use of highly enriched nuclear fuel, so as to not incur on potential delays completely beyond its control in order to obtain the associated special authorizations.

B. NASA should give priority to commercial procurement practices.

The results of the risk assessments and simulations are shown in cumulative distribution function (CDF) or, when appropriate, in complementary cumulative distribution function (CCDF) form, for the three alternatives mentioned earlier, A7, A8, and A9, in Figure 3-7 thru Figure 3-11. The CDF form, which directly shows the probability that a parameter outcome be less than some predefined value, is preferable for visualizing parameter distributions where the "direction of goodness" is from lower to higher values of the parameter of interest. In such cases, risk is associated with the probability that the alternative outcome for a parameter of interest may be "too low" with respect to the goals that mission designers are aiming for. In our example this is the case for the PMS and ESDR KPMs. Conversely, the CCDF form, which directly shows the probability that a parameter outcome be greater than some fixed value, is more convenient for identifying the risk that a KPM outcome may be "too high." This is the case for KPMs PRR, PC, and TLR.

It should be noted that, for the parameters affected by the pre-definition of fixed constraints not to be exceeded or undershot – which in our example is assumed to be the case for the PRR, PC, and TLR KPMs – the figures show the risk that such constraints be violated by some amount. Predefined constrains usually translate into the definition of corresponding firm requirements at an activity execution stages.

For all KPMs, the information in the figures include the "risk-normalized values" of the parameters of interest that correspond to an assumed quantitative level of risk tolerance, which in the figures is identified as a quantitative risk tolerance level (RTL). The considerations that lead to the definition of a RTL for each of the KPMs have been preliminarily discussed in their general qualitative form in Section 3.2.1, and are further discussed in more detail below, in Section 3.2.7. It is noted that, once an alternative is identified as the preferred option, and selected for formalization into an activity or project at execution stage, the PM risk-normalized values corresponding to the desired levels of risk tolerance are to be used as reference values for the discussion and definition of formalized performance requirements and goals that takes place within the activity-executing organizations and, as applicable, more specifically in the negotiations between the ***Acquirer*** and ***Provider*** entities.

The CDF and CCDF results shown in the figures are purely notional. The Monte Carlo estimation analyses required to carry out actual calculations of KPM outcomes are in general rather complex, and in the case of our example out of scope with respect to the tutorial nature of this handbook.

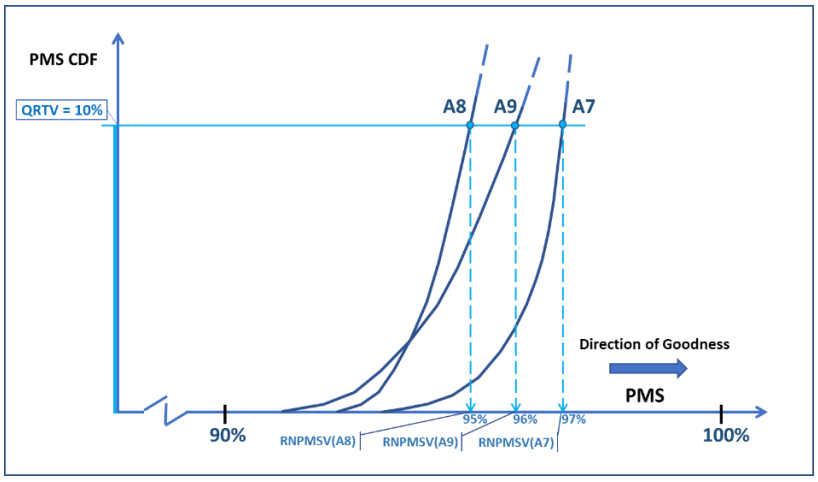


Figure 3-7. PMS Cumulative Distribution Functions and Risk-Normalized Values of Alternatives

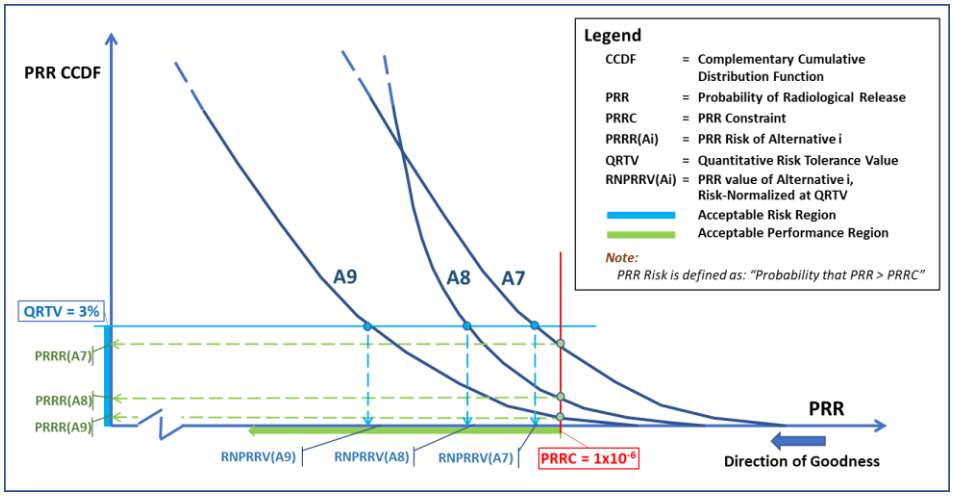


Figure 3-8. PRR Complementary Cumulative Distribution Functions, Constraint Risks, and Risk-Normalized Values of Alternatives

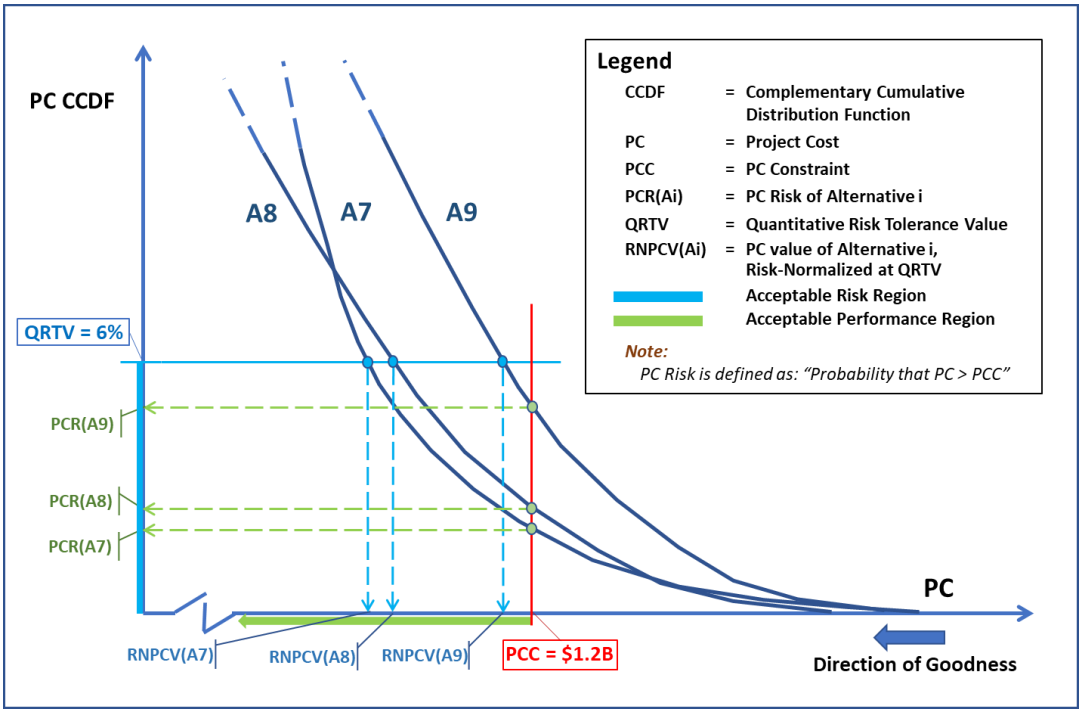


Figure 3-9. PC Complementary Cumulative Distribution Functions, Constraint Risks, and Risk-Normalized Values of Alternatives

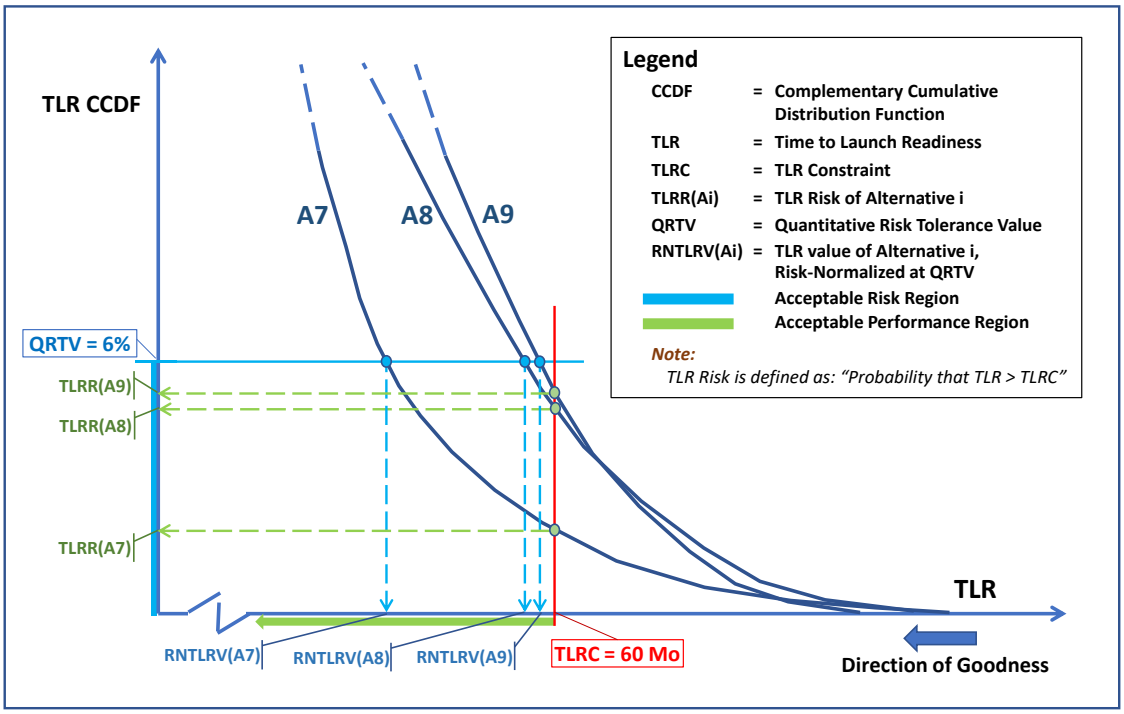


Figure 3-10. TLR Complementary Cumulative Distribution Functions, Constraint Risks, and Risk-Normalized Values of Alternatives

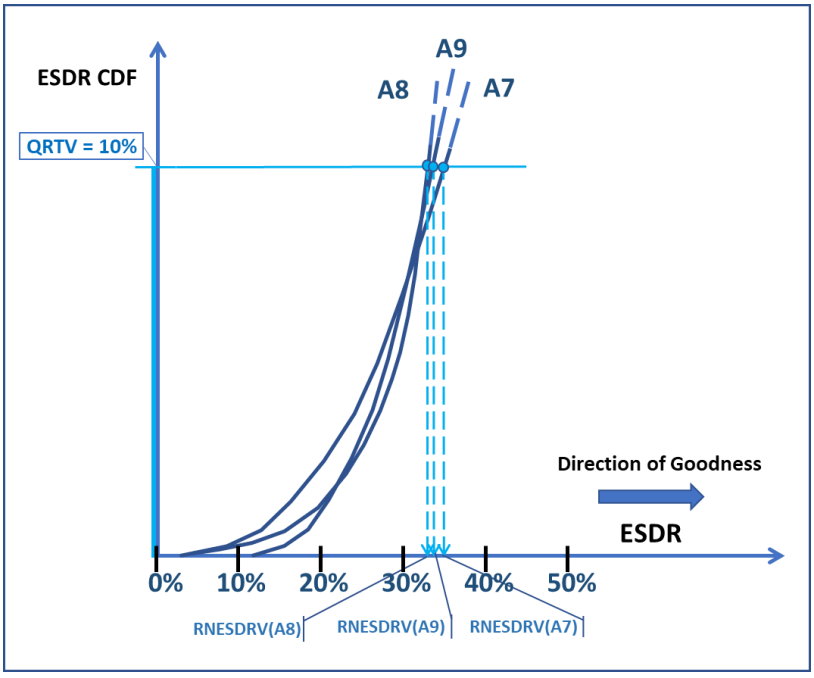


Figure 3-11. ESDR Cumulative Distribution Functions and Risk-Normalized Values of Alternatives

A summary explanation of the results of the risk profile estimations presented in the above figures can be given as follows:

Probability of Mission Success (PMS) Ranking:

Alternative 7 has the highest predicted risk-normalized value of PMS, i.e., the lowest PMS risk at the assumed RTL; Alternative 8 presents the lowest risk-normalized PMS value primarily because of the risk associated with on-orbit RPM assembly; Alternative 9 shows an in between risk-normalized value because it transfer the risk associated with executing the RPM assembly on Planet X to a follow-up mission; in addition the twin spacecraft split RPM delivery permits consideration and execution of a "recovery mission" with a spare RPM module if one of the baseline delivery missions were to fail.

Probability of Radiological Release (PRR) Ranking:

Alternative 7 is has the lowest risk-normalized PRR value because it carries both Radioisotope Thermoelectric Generator (RTG) release risk and RPM accidental criticality risk; Alternative 8 carries RTG risk in split mode between two launches, and limited accidental criticality risk (i.e., only after RPM on-orbit assembly, if a reentry accident occurs); Alternative 9 only carries RTG risk, split between two launches.

Project Cost (PC) Ranking:

Alternatives 7 and 8 have similar risk-normalized costs because the cost of an NHLV is more than double that of two CMLVs, therefore the two costs are predicted to be similar despite the fact that for Alternative 8 the assembly in orbit process is predicted to add more cost to the mission than what is expected for an RPM assembly on the ground; Alternative 9 has a somewhat higher risk-normalized cost than either Alternative 7 or 8 because it requires two interplanetary spacecraft, although smaller and cheaper than the single large one required for the other two alternatives; the Alternative 9 cost is only moderately higher because the cost risk of the Planet X RPM assembly operation is transferred "out of scope," to a follow-up mission.

Time to Launch Readiness (TLR) Ranking:

Alternatives 8 and 9 have similar TLR risk-normalized values that are higher than the corresponding value for Alternative 7, because they both require planning and executing two launches instead of just one.

Expert Staff Development Ratio (ESDR) Ranking:

No significant difference exists between the ESDR risk-normalized values for the three alternatives.

3.2.7 Define Mission Risk Posture with Recommended Risk Tolerances

The ensemble of risk tolerance values that decision makers indicate to be applicable to a mission KPM set reflects and quantitatively defines the project and mission risk posture. Risk tolerances are applied in the evaluation of alternatives in distinct ways, as discussed in Part 1, Sections 4.9.2.1 and 4.9.2.2, depending on whether they are being used to evaluate alternatives with respect to a PM for which no hard constraint exists, or otherwise for one affected by the pre-establishment of

such a constraint. In either case, the decision maker indicates the risk tolerance value as the quantile or percentile of the PM or KPM probability distribution function that is to be used to compare the mission alternatives being considered. If a hard constraint (plus or minus any margin) is set for a KPM, only the alternatives for which the indicated risk tolerance quantile / percentile falls on the "good side" of the constraint (+/- margin value) are considered admissible and included in a relative comparison.

For the example considered, three of the five KPM used in the RIDM AoA are assumed to be affected by pre-defined constraints, i.e.:

- PRR, the Probability of Radiological Release, must be < 1 in 1,000,000 to keep the mission at the NSPM-20 Tier II Level of scrutiny and approval
- PC, the Project Cost, must be < $ 1.2B
- TLR, the Time to Launch Readiness, must be < 60 mos

For the above KPMs, it is also noted that the "direction of goodness" goes in the opposite direction of magnitude, i.e., lower values of the parameters indicate better performance. The remaining two PMs designated as KPMs, i.e., PMS, Probability of Mission Success, and ESDR, Expert Staff Development Ratio, are assumed not to be assigned pre-established constraints. Their "direction of goodness" goes in the same direction of their magnitude, i.e., higher values of the parameters indicate better performance.

For the set of five KPMs, it is recalled that, as per rationales provided at the end of Section 3.2.1, it is assumed that the project decision makers have converged on, and communicated to the risk analysts, a flexible risk posture, with risk tolerance criteria that vary in strictness across the set, as indicated by Table 3-V below.

Table 3-V. Example of Qualitative and Quantitative Risk Tolerance Definitions Reflecting Planet X Mission and Project Risk Posture

KPM	Decision Makers' Qualitative Risk Tolerances	Quantitative Risk Tolerance
PMS	medium risk tolerance	10%
PRR	very low risk tolerance	3%
PC	low risk tolerance	6%
TLR	low risk tolerance	6%
ESDR	medium risk tolerance	10%

The table also shows the quantitative risk tolerance levels (RTLs) that correspond to the interpretation our example assumes to be given by the project RIDM analysts to the qualitative indications received from the decision makers. Regarding this, it is noted that there exists no prescriptive rule for how a qualitative indication of risk tolerance may be translated into an RTL. Rather, in an actual project setting it may be expected that a convergence between decision makers' desires, expressed in qualitative form, and analysts' selection of quantitative values (the RTLs) reflecting such directives, will occur via an iterative process of "trial and error." Regardless of the specific course that such a process may follow, it may well result in correspondences between

qualitative attributes and quantitative values of risk tolerance not resembling the notional example of such a correspondence provided by Table 3-V.

3.2.8 Compare Risk Profiles, Recommend an Alternative, and Document the Rationale

Table 3-VI gives a quick-view summary of the relative ranking of the alternatives in each of the five KPM dimensions of interest, as emerging from the quantitative analysis results presented earlier in Figure 3-7 through Figure 3-11. The table also contains, in terms fully consistent with the explanation provided earlier in Section 3.2.7, the explanation of why the quantitative CDF and CCDF KPM results are as depicted in the figures.

Table 3-VI. Relative Ranking of Alternatives by KPM

KPMs	Relative Ranking of Alternatives by KPM			Explanation
	A7	A8	A9	
PMS	1	3	2	Alternative 7 has the highest predicted PMS / lowest PMS risk; Alternative 8 is ranked lowest primarily because of the risk associated with on-orbit RPM assembly; Alternative 9 is ranked second because it transfer the risk associated with RPM on Planet X assembly to a follow-up mission; in addition the twin spacecraft split RPM delivery permits consideration and execution of a "recovery mission" with a spare RPM module if one of the baseline delivery missions were to fail.
PRR	3	2	1	A7 carries both RTG release risk and RPM accidental criticality risk; A8 RTG risk is split between two launches and A8 carries limited accidental criticality risk (only after on-orbit assembly, if a reentry accident occurs); A9 only carries RTG risk, split between two launches.
PC	1	1	2	A7 and A8 have similar cost because NHLV cost is more than double that of two CMLVs, therefore the two costs are predicted to be similar despite the fact that for A8 the assembly in orbit maneuver does add to the mission cost in comparison to assembly on the ground; A9 is somewhat more costly because it requires two interplanetary spacecraft, although smaller and cheaper than the single large one required for the other two alternatives; in addition A9 saves in cost by pushing RPM assembly operation costs "out of scope," to a follow-up mission.
TLR	1	2	2	A8 and A9 have similar higher TLR risk in comparison to A7 because they require two launches instead of one.
ESDR	1	1	1	No significant difference exists between the three alternatives.

Based on the relative rankings of the alternatives shown in the table, and the risk profiles presented earlier in the figures included in Section 3.2.7, a recommendation of "preferred alternative" can be deliberated, documented, and submitted to the project and mission decision makers. In many cases a recommendation may be identified based on the greater or lesser "weight" (i.e., relative importance) that the analysts believe should be given to certain KPMs, I others. This may be gleaned from the "risk posture profile," i.e., the different attributes of risk tolerance that the project decision makers and stakeholders have assigned to different KPMs.

In the example considered, given the "Very Low" risk tolerance assigned to the PRR KPM, and the moderate degree of risk disadvantage that Alternative 9 has in the other KPM dimensions

where it is not the best ranked alternative, the analysts may deliberate that there is a strong rationale for recommending it as the preferable alternative. Under such assumptions, the risk informed conclusion of the Activity-Planning RIDM would thus be to recommend a NPSPD overall mission execution based on the separate launches of two RTG-powered, relatively small spacecraft carrying separate RPM submodules to Planet X. The two launches would use two commercial medium-lift launch vehicles (MLVs) procured via launch service contracts. The RPM submodules delivered to Planet X in this fashion would then be later assembled on Planet X as part of an RPM activation process planned within the scope of a follow-on power production and utilization demo mission. As mentioned earlier, this recommended mission alternative transfers the risk associated with any potential issues in the execution of the RPM module assembly on Planet X to a later mission, which is assumed to be planned as part of an overall campaign to set up a Planet X semi-permanent base.

Documentation of the deliberation and final recommendation should include, in summary form, all of the following:

- The definitions of the project and mission objectives
- The considerations pertaining to project risk posture
- The definitions of the project and mission design alternatives
- The identification of project / mission PMs and KPMs
- A description of the risk analysis models for the project and mission alternatives, and of the associated assumptions
- The RIDM risk analysis results
- The definition of risk tolerances
- The rationale for the deliberated project / mission alternative recommendation(s).

3.3 References for Chapter 3

1. Kjærulff U.B. and Madsen A.L, “Bayesian Networks and Influence Diagrams: A Guide to Construction and Analysis,” Springer, 2008.

4 Examples of CRM Execution

This chapter illustrates the CRM process by focusing on two specific organizational entities. The first is a hypothetical project designated as Project "X", and the second a hypothetical center designated as Center "Y". Project "X" is a shorthand notation that is synonymous with the activity referred to in Chapters 2 and 3 (starting in Section 2.3.1) as the "*Nuclear Planetary Surface Power Delivery Mission*," or, in short, the "*NPSPD Mission.*"

The overall objective for Project "X" is to set up a nuclear fission reactor on the surface of an extraterrestrial planet or one of its moons, designated generically in this example as Planetary Mass "X". The ultimate aim is to provide power for a future colony of humans on the planetary object, although the example proceeds only to the point of having the ability to provide power prior to such colonization. The mass is postulated to be very distant from Earth, in the outer reaches of the solar system, and is considered to have an atmosphere that could be used to facilitate orbital capture of the spacecraft via the technique of aerobraking, (Saturn's moon Titan would be an existing example of such an object; hence the use of the term "planetary mass" rather than simply "planet".) The project priority is a part of the overall development of a space nuclear system capability discussed earlier in Section 2.1.1.1. Of the various program/project objectives presented in that section, Project "X" specifically addresses Objective C-1: "Enable Nuclear Surface Power Utilization in a Planetary Mission."

Consistent with the results of the Activity-Planning RIDM analysis and deliberations discussed in Chapter 3, and in particular with Alternatives A6 and A9 in Table 3-IV, the NASA authorities have determined that the nuclear fission reactor will contain only moderately enriched uranium (<20%) and will be transported from the surface of Earth directly to the surface of Planetary Mass "X" in multiple trips. (Note that in Chapter 3, the number of multiple trips was specifically taken to be two, whereas in this chapter, the number of trips is allowed to be greater than two if it is found that more trips are needed to satisfy the objectives of Project "X".) Each launch from Earth will utilize a commercial medium-lift launch vehicle (CMLV), and each flight to the planetary mass will take place in a spacecraft carrying one or more nuclear reactor power modules (RPMs) and needed equipment. The modules, which will be provided by under the supervision of the Department of Energy working together with a commercial company, will be collected at the destination to be assembled robotically or by astronauts in a future mission.

In addition, consistent with Section 3.2.6 and Table 3-VI, the spacecraft's electrical power needs during space transport, orbital insertion, and payload separation will be provided by conventional radioisotope thermoelectric generators (RTGs). Also, each spacecraft will be instrumented with high-tech atmospheric sensing devices to assist the aerocapture maneuver that will be used to achieve orbit around the planetary mass.

In this chapter, the teams develop methods and obtain results in the following areas:

- Developing risk statements using a standardized format
- Analyzing and ranking individual risk scenarios, using both probabilistic and heuristic approaches

- Aggregating individual risk scenarios in order to determine the aggregate risk to an affected objective, using both probabilistic and heuristic approaches
- Conducting Activity-Execution RIDM using both probabilistic and heuristic approaches

4.1 Baselining the Entity Objectives and Risk Posture

The objectives of Center "Y", in this example, involve two separate but related priorities. One is to provide the institutional support needed to ensure the success of the project, i.e., the set-up of a nuclear fission reactor to provide electric power on Planetary Mass "X". This objective involves having the necessary resources, in terms of staffing, facilities, and materials, through a combination of internal capability development, cooperation with the Department of Energy (DOE), and external procurements. The objective just mention encompasses three objectives previously listed in Section 2.1.1.1, namely C-1.1, C-1.2, and C-1.3.

The other priority is to develop and maintain a core competency in a particular area, assigned to it by the Agency, that can be utilized by all organizations within the Agency. The particular area of core competency considered to be the responsibility of Center "Y" in this chapter is the development and maintenance of cutting-edge expertise in cybersecurity. This responsibility addresses a long-term need for Agency expertise in protecting against cyberattack, and is separate from (although related to) the shorter-term need for providing cybersecurity for Project "X". Both the shorter-term and the longer-term cybersecurity needs are addressed by Center "Y", but the former is considered to be a project support objective and the latter an Agency-wide core competency objective.

Table 4-I through Table 4-III provide a listing of the objectives to be pursued by Project "X" and Center "Y", along with the corresponding performance measures that will be used to measure the degree to which the objectives are met. They are somewhat different, and more extensive, than those of Table 3-I. This reflects the elaboration of entity-level top objectives into sub-objectives as the activity goes from pre-formulation to formulation, as well as the need for comprehensiveness in CRM, as compared to RIDM, where the crucial performance attributes to consider are those that distinguish among the alternatives. The relationship between the directly-assessed objectives of Table 4-I through Table 4-III and the higher-level Project "X" and Center "Y" objectives from which they derive is relevant to the aggregation of risk from lower to higher levels of an objectives hierarchy.

Table 4-I. Project "X" Objectives and Performance Measures

Objec. No.	Entity Objective	Perf. Meas. No.	Performance Measure
X1	Ensure that the delivered nuclear reactor power capacity meets the needs for a future colony	X_PM1	Delivered nuclear reactor power capacity (kW)
X2	Ensure that the probability of loss of mission from an accident does not exceed the minimum expectation	X_PM2	Probability of loss of mission, P(LOM)
X3	Ensure that the delivered nuclear reactor reliability meets the needs for a future colony	X_PM3	Delivered nuclear reactor reliability
X4	Ensure public safety during lift-off and ascent from Earth	X_PM4	Probability of a catastrophic accidental ascent failure resulting in public exposure
X5	Prevent planetary mass contamination during the aero-capture maneuver, landing, and surface operations	X_PM5	Probability of a catastrophic failure during entry to Planetary Mass "X" resulting in radioactive contamination of the planetary mass
X6	Ensure that the project Information Technology (IT) networks and databases are protected against theft of sensitive data	X_PM6	Conditional probability of sensitive data disclosure given occurrence of a cyberattack
X7	Utilize pooled assets administered by the Mission Support Directorate Shared Services Center when practical and efficient for the Planetary Mass "X" surface nuclear reactor placement project	X_PM7	Avoidance of duplication of efforts during Project "X", as rated by elicitation of experts (e.g., score of 1 to 10)
X8	Stay within the schedule allocated to the project throughout its duration	X_PM8	Time to project completion (months)
X9	Stay within the budget allocated to the project throughout its duration	X_PM9	Cost to completion ($M)

Table 4-II. Center "Y" Project Support Objectives and Performance Measures

Objec. No.	Entity Objective	Perf. Meas. No.	Performance Measure
Y1	Communicate effectively with technical personnel from DOE and a commercial partner to develop the nuclear reactor and RTG electric conversion system	Y_PM1	Effectiveness of communication protocols and data sharing as measured by periodic audits (e.g., score of 1 to 10)
Y2	Ensure sufficient test facility availability to satisfy the needs of the Planetary Mass "X" surface nuclear reactor placement project	Y_PM2	Facility availability over the period of performance (% of time)
Y3	Provide technical staff and other resources to support the Planetary Mass "X" surface nuclear reactor placement project	Y_PM3	Projected availability of technical staff at a specified time in the future (Full Time Equivalents (FTEs))
Y4	Utilize pooled assets administered by the Mission Support Directorate Shared Services Center when practical and efficient for the Planetary Mass "X" surface nuclear reactor placement project	Y_PM4	Avoidance of duplication of efforts during support of Project "X", as rated by elicitation of experts (e.g., score of 1 to 10)
Y5	Stay within the schedule allocated to the center for project support	Y_PM5	Time to completion of tasks (months)
Y6	Stay within the budget allocated to the center for project support	Y_PM6	Time to project completion (months)

Table 4-III. Center "Y" Objectives and Performance Measures for New Technologies, Core Competencies, and Imposed Mandates

Objec. No.	Entity Base Objective	Perf. Meas. No.	Performance Measure
YY1	Utilize pooled assets administered by the Mission Support Directorate Shared Services Center when practical and efficient for the development and maintenance of the cybersecurity core competency	YY_PM1	Avoidance of duplication of efforts in the cybersecurity core competency development activity, as rated by elicitation of experts (e.g., score of 1 to 10)
YY2	Maintain sufficient availability of existing senior level cybersecurity specialists to develop and maintain the agency-wide cybersecurity core capability	YY_PM2	Projected availability of existing senior level cybersecurity specialists at a specified time in the future (FTEs)
YY3	Maintain sufficient availability of junior level cybersecurity specialists to make up for anticipated shortage of senior level cybersecurity specialists	YY_PM3	Projected availability of new junior level cybersecurity specialists at a specified time in the future (FTEs)
YY4	Maintain sufficient availability of training courses in cybersecurity technology	YY_PM4	Projected availability of training courses in cybersecurity technology at a specified time in the future (no. of courses)
YY5	Develop and maintain a cybersecurity laboratory that fosters research and development of novel cybersecurity concepts that protect against cyberattack but do not compromise the operational performance of the Agency by hindering communication	YY_PM5	Laboratory coverage of long-term cybersecurity R&D needs, as measured by elicitation of experts (e.g., score of 1 to 10)
YY6	Stay within the schedule allocated to the center for developing and maintaining the cybersecurity core competency	YY_PM6	Time to completion of cybersecurity core competency development (months)
YY7	Stay within the budget allocated to the center for developing and maintaining the cybersecurity core competency	YY_PM7	Cost to completion of cybersecurity core competency development ($M)
YY8	Ensure timely and effective accommodations for people with disabilities in accordance with all Federal and NASA requirements	YY_PM8	Percentage of cases that meet the 30-day timeframe in NPR 3713.1C (2019) for resolution of accommodation requests for individuals with disabilities and religious accommodation requests

Table 4-IV through Table 4-VI provide the cognizant managers' sets of performance markers and risk tolerance levels associated with each performance measure. In all cases, the managers have chosen to define two markers for each objective: a performance requirement (PMK-R) and a performance goal (PMK-G). Associated with these markers are the risk tolerance levels RTL-R and RTL-G, respectively. These values have been specified by NASA management at the

appropriate level, informed by the RIDM analysis as well as from input from external and internal stakeholders, and have been incorporated into the program/project and center plans. The risk tolerance levels differ from those used for risk normalization during RIDM (e.g., as shown in Table 3-V), reflecting the refinement of risk attitudes as the activities go from pre-formulation to formulation. The values in the tables, of course, are hypothetical, intended for illustration purposes only, and not correlated with any existing program/project or center plan.

Table 4-IV. Example Performance Measures and Hypothetical Performance Markers and Risk Tolerance Levels for Project "X" Programmatic Objectives

Project "X" Performance Measure	PMK-G	PMK-R	RTL-G	RTL-R
X_PM1 : Delivered nuclear reactor power capacity (kW)	100 kW	85 kW	10 %	5 %
X_PM2 : Probability of loss of mission, P(LOM)	0.005 (1 in 200)	0.01 (1 in 100)	50%	25%
X_PM3 : Delivered nuclear reactor reliability	0.99	0.98	50 %	25 %
X_PM4 : Probability of a catastrophic accidental ascent failure resulting in public exposure	0.001 (1 in 1000)	0.002 (1 in 500)	50 %	25 %
X_PM5 : Probability of a catastrophic failure during entry to Planetary Mass "X" resulting in radioactive contamination of the planetary mass	0.005 (1 in 200)	0.01 (1 in 100)	50%	25%
X_PM6 : Conditional probability of sensitive data disclosure given occurrence of a cyberattack	0.05	0.10	20 %	10%
X_PM7 : Avoidance of duplication of efforts during Project "X", as rated by elicitation of experts (scale of 1 to 5)	0.50	1.00	50 %	25 %
X_PM8 : Time to project completion (months)	60	72	6 %	3 %
X_PM9 : Cost to completion ($M)	$ 1.25B	$ 1.38B	30 %	15 %

Table 4-V. Example Performance Measures and Hypothetical Performance Markers and Risk Tolerance Levels for Center "Y" Project Support Objectives

Center "Y" Project Support Performance Measure	PMK-G	PMK-R	RTL-G	RTL-R
Y_PM1 : Effectiveness of communication protocols and data sharing as measured by periodic audits (scale of 1 to 10)	8 out of 10	7 out of 10	10%	5%
Y_PM2 : Test facility availability over the period of performance (% of time)	90%	80%	10 %	5 %
Y_PM3 : Projected availability of Safety and Mission Success (SMS) technical staff at a specified time in the future (FTEs)	20 FTEs	15 FTEs	10%	5%
Y_PM4 : Fraction of effort not provided by Mission Support Directorate (MSD) Shared Services	0.50	1.00	50 %	25 %
Y_PM5 : Time to completion of tasks (months)	60	72	6 %	3 %
Y_PM6 : Cost to completion of tasks ($B)	$ 1.25B	$ 1.33B	30 %	15 %

Table 4-VI. Example Performance Measures and Hypothetical Performance Markers and Risk Tolerance Levels for Center "Y" New Technology and Core Competency Development Objectives

Center "Y" Performance Measures for Technology Development, Core Competencies, or Imposed Mandates	PMK-G	PMK-R	RTL-G	RTL-R
YY_PM1 : Fraction of effort not provided by MSD Shared Services	0.20	0.40	50 %	25 %
YY_PM2 : Projected availability of existing senior level cybersecurity specialists at a specified time in the future (FTEs)	20 FTEs	16 FTEs	40 %	20 %
YY_PM3 : Projected availability of junior level cybersecurity specialists at a specified time in the future (FTEs)	20 FTEs	16 FTEs	40 %	20 %
YY_PM4 : Projected availability of training courses in cybersecurity technology at a specified time in the future (no. of courses)	10 courses	7 courses	20 %	10 %
YY_PM5 : Laboratory coverage of long-term cybersecurity R&D needs, as measured by elicitation of experts (scale of 1 to 10)	8 out of 10	7 out of 10	40 %	20 %
YY_PM6 : Time to completion of cybersecurity core competency development (months)	84	96	6 %	3 %
YY_PM7 : Cost to completion of cybersecurity core competency development ($M)	$ 70M	$ 80M	30 %	15 %
YY_PM8 : Percentage of cases that meet the 30-day timeframe in NPR 3713.1C (2019) for resolution of accommodation requests for individuals with disabilities and religious accommodation requests	80 %	50 %	30 %	15 %

4.2 Identification of Individual Risk Scenarios

The identification of individual risk scenarios depends on the performance measures to which it applies and on knowledge about the types of risks that tend to affect the achieved value of the performance measures. The hypothetical project and center risk management analytical teams in this example access the latter by tapping into the collective experience of persons throughout the Agency that have been heavily involved with major programs/projects and/or with major institutional initiatives. Their thesis is that problems that have occurred during previous major activities, together with knowledge about current developments within the Agency, can help elucidate individual risk scenarios that have a high potential for affecting ongoing or future major activities.

To produce the example individual risk scenarios which follow, the RM analytical teams utilize a variety of sources including the August 2021 Office of Safety and Mission Assurance (OSMA) Risk Management Quarterly Reporting Cycle Executive Overview [1], which provides the results of a survey of NASA's centers and facilities regarding the risks that are of most concern to them. Following is a brief summary of four types of risk that appeared most often in the responses to the survey:

- Unanticipated inability to replace aging infrastructure or equipment due to funding reductions or realignments
- Unanticipated obsolescence of infrastructure or equipment due to changes in Agency goals or requirements
- Unanticipated staff or leadership attrition due to retirements or competing opportunities
- Unanticipated mandates from above without prior communication or coordination

While these risks tended to be institutional in nature, owing to the nature of the survey, some of the responses involved programmatic hazards. In addition, there are other sources of information that focus on programmatic risks, including the evaluations of past and present program/project effectiveness by outside organizations such as the General Accounting Office (GAO), and by independent inside organizations such as the Office of Inspector General (OIG). Using these sources of information, the RM analytical team compiles a list of risk scenarios that they deem to be appropriate for the base objectives listed in Table 4-I through Table 4-III.

Per NPR 8000.4C and Part 1 of this Handbook, the individual risk scenarios are summarized using formatted risk statements (slightly rearranged here from the original for convenience):

> *Given that **[Condition]**, there is a possibility of **[Departure]**, which can result in **[Consequence]**, adversely impacting **[Asset]** and the achievement of **[Affected Objective(s)]**.*

Table 4-VII and Table 4-VIII, below, provides the elements of 6 example risks statements developed by the teams, organized in terms of the most significantly affected objective.

Table 4-VII. Example Risk Statement Elements most significantly affecting Project "X" Objective X2: Ensure that the probability of loss of mission from an accident does not exceed the minimum expectation

Risk No.	Risk Scenario Synopsis	*[CONDITION]*	*[DEPARTURE]*	*[CONSEQUENCE]*	*[ASSET/ OBJECTIVE]*
X_RS1	A nuclear reactor development test indicates power-to-weight ratio less than expectation	Although the use of nuclear fission reactors in space has been shown to be feasible, there have been no demonstrations yet for reactors big enough to produce the amount of power needed to support a human colony on Planetary Mass "X"	Testing of larger reactors in space-like environments may show that the reactor power-to-weight ratio is less than expected	Not enough surface reactor capacity to provide the needed power for Planetary Mass "X"	Asset: Surface nuclear fission reactor. Objective: *X2*
X_RS2	Shortages of Pu^{238} for RTGs limits the number of flights, thereby limiting the number of reactor modules that can be transported to Planetary Mass "X"	1. The supplies of Pu^{238} are dwindling 2. There is growing political opposition in Congress to producing Pu^{238} domestically 3. Foreign sources of Pu^{238} are unpredictable	Not being able to procure enough Pu^{238} to power the spaceflights needed to transport all the reactor modules	Not enough surface reactor capacity to provide the needed power for Planetary Mass "X"	Asset: Surface nuclear fission reactor. Objective: *X2*
X_RS3	The TLM Liquid Oxygen (LOX)/methane engine is not matured to its target reliability	Prototype LOX/methane engine vacuum tests indicate the presence of unanticipated combustion instability	The target LOX/methane engine ignition reliability is not achieved	Decreased probability of successfully delivering the reactor to the surface of Planetary Mass "X"	Asset: LOX/methane engine. Objective: *X2*
X_RS4	Thrust oscillation damages the surface nuclear fission reactor	Finite element models show an unexpected coupling between the launch vehicle thrust oscillation and the structural vibration modes of the integrated vehicle	Vibration-induced damage to the surface nuclear fission reactor during launch	Inoperability of the delivered surface nuclear fission reactor	Asset: Surface nuclear fission reactor. Objective: *X2*

Table 4-VIII. Example Risk Statement Elements most significantly affecting Center "Y" Objective Y2: Ensure sufficient test facility availability to satisfy the needs of the Planetary Mass "X" surface nuclear reactor placement project

Risk No.	Risk Scenario Synopsis	*[CONDITION]*	*[DEPARTURE]*	*[CONSEQUENCE]*	*[ASSET/ OBJECTIVE]*
Y_RS1	Competition for the Center "Y" test facility delays Project "X" technology maturation	Additional projects are in formulation that will need to use the test facility	The Center "Y" test facility is unavailable to Project "X"	Delays in developing the Project "X" technologies that are dependent on Center "Y" testing for maturation, affecting Project "X" cost and schedule objectives	Asset: Project "X" success. Objective: *Y2*
Y_RS2	Increasing unavailability of Center "Y" test facility due to facility aging	Increasing rate of Center "Y" test facility component failures and increasing repair downtimes due to facility aging	Test facility unavailability exceeds acceptable limits	Delays in developing the Project "X" technologies that are dependent on Center "Y" testing for maturation, affecting Project "X" cost and schedule objectives	Asset: Project "X" success. Objective: *Y2*

4.3 Analysis and Ranking of Individual Risk Scenarios

As discussed in Part 1 of this handbook, NPR 8000.4 [2] stresses:

> "*When possible, quantitative characterizations of performance and corresponding risk levels are preferable, as they more directly enable risk vs. benefit 'analysis of alternative' (AoA) evaluations that constitute the foundation of the RIDM support to decision making.*"

Correspondingly, this handbook stresses the importance and value of managing risk quantitatively, using a "probabilistic" approach to risk analysis, aggregation, and decision-making. Nevertheless, given the practical limits within which any risk management activity must take place, there is a potential need for more qualitative or "heuristic" approaches when more rigorous probabilistic methods are impractical due to limits of time, resources, or data, recognizing that the results of such methods may differ from those of more rigorous methods. Therefore, the analysis and ranking of individual risk scenarios presented in this section is partitioned into two subsections, one presenting a probabilistic approach and another presenting a heuristic approach.

4.3.1 Probabilistic Approach

In a probabilistic approach, models are developed to quantitatively estimate the effects of individual risk scenarios on the affected performance measures. To illustrate the application of a probabilistic approach to analyzing individual risk scenarios, risks X_RS3 and X_RS4 from Table 4-VII are used.

4.3.1.1 Analysis and Classification of Individual Risk Scenario X_RS3, The In-Space LOX/Methane Engine is Not Matured to its Target Reliability

The risk statement for risk X_RS3 is:

> *Given that prototype LOX/methane engine vacuum tests indicate the presence of unanticipated combustion instability, there is a possibility that the target LOX/methane engine ignition reliability is not achieved, thereby leading to decreased probability of successfully delivering the reactor to the surface of Planetary Mass "X", adversely impacting LOX/methane engine and the achievement of Objective X2, "Ensure that the probability of loss of mission from an accident does not exceed the minimum expectation."*

Figure 4-1 shows a risk scenario diagram (RSD) for risk X_RS3 that is integrated into the intended path of the baseline plan, consistent with Figure 5-6 of Part 1 of this handbook. Figure 4-1 is simpler than Figure 5-6 of Part 1 because it assumes that there are no existing contingencies for responding to the situation in which the LOX/methane engine reliability has not been matured to meet specifications (which have been flowed down from Objective X2). In general, this is to be expected from newly identified individual risk scenarios, since such risks haven't cycled through the CRM *Plan* step yet and are therefore uncontrolled by any specifically designed preventive or mitigative features.

The right-hand side of Figure 4-1 illustrates the results of the probabilistic analysis. Overall:

- The current project status includes the condition that motivated the identification of risk X_RS3, namely the combustion instability observed in vacuum engine tests.
- The departure event, failure to achieve the target LOX/methane engine ignition reliability (DE_{X_RS3}), will occur if Project "X" cannot successfully eliminate the combustion instability. The probability of occurrence of DE_{X_RS3} is evaluated based on the expert judgement of the propulsion engineers and their assessment of the magnitude of the challenge presented by the combustion instability issue. Elicitation of such information would be facilitated by the project risk analysts.
- The nominal probability of reactor delivery to Planetary Mass "X" (i.e., the top end state) is assessed using mission risk analysis techniques such as probabilistic risk assessment (PRA), applied to the nominal mission. The nominal output of such a mission risk analysis is a probability density function (pdf) that accounts for epistemic uncertainties. Because it is used here for the purpose of analyzing an individual risk scenario in isolation from other individual risk scenarios, the only epistemic uncertainties represented in the analysis are those that have been accepted. Parameters whose uncertainties count as risks are set at nominal point values such as their means (parameters other than those associated with the individual risk scenario being analyzed, of course).

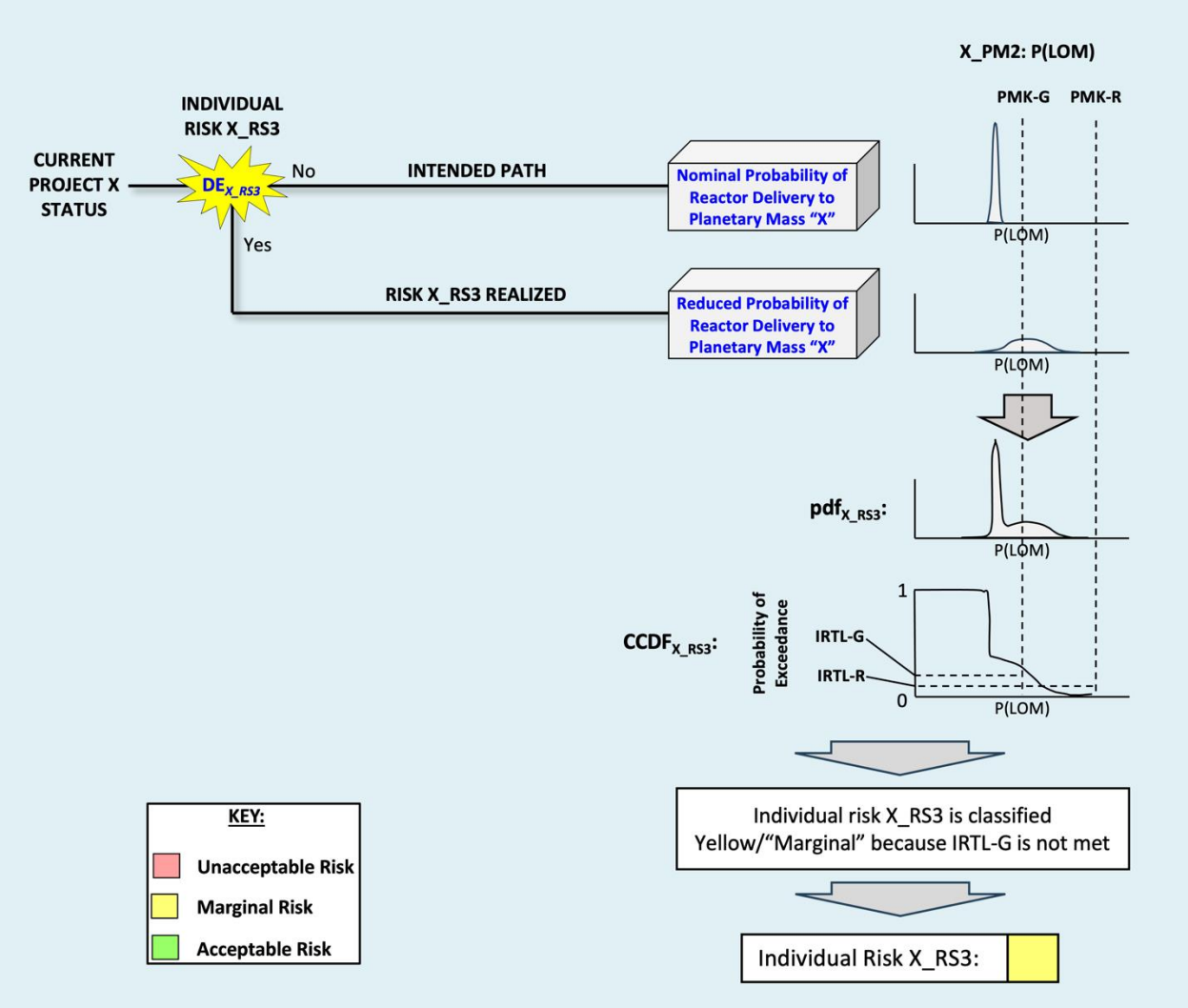


Figure 4-1. Probabilistic Analysis of Individual Risk Scenario X_RS3 (notional)

- In general, each PM defined for Project "X" will have a performance model developed for it as an essential tool of program management. These performance models are developed by the project's relevant subject matter experts. They are key resources that can be leveraged for risk management purposes by modifying them as needed to reflect the circumstances associated with each RSD end state. In the case of the nominal end state, the existing mission risk analysis directly addresses nominal P(LOM) without the need for modification.
- The reduced probability of reactor delivery to Planetary Mass "X" (the bottom end state) can be assessed using the mission risk analysis, suitably modified to reflect the reduced LOX/methane engine reliability resulting from the realization of individual risk scenario X_RS3. The reduced reliability itself would likely come from an analysis of the vacuum test data and could have significant epistemic uncertainty associated with it. For example, if the mission risk analysis is a PRA, and that PRA has a basic event, *benign LOX/methane engine failure*, then a suitable modification might be to replace the nominal *benign*

LOX/methane engine failure basic event with one that has a higher mean probability and a larger error factor consistent with the problematic test results. The pdf accompanying the end state shows the output from the modified mission risk analysis.

- The relative sizes of the two pdfs discussed above reflect the relative probabilities that the associated end states will occur. In this RSD, which only has one branch point, DE_{X_RS3}, the area under the nominal pdf equals the probability that DE_{X_RS3} does not occur, whereas the area under the pdf for the realized risk equals the probability that DE_{X_RS3} does occur. This enables the two pdfs to be combined into a single overall pdf for individual risk scenario X_RS3 that reflects its probability of being realized.
- The pdf and CCDF below the end state pdfs represent the assessment of performance measure X_PM2 in the presence of individual risk scenario X_RS3 (and only X_RS3). The pdf is constructed by summing the end state pdfs. In other words, the value of the pdf at a given value of P(LOM) is just the sum of the values of the end state pdfs at that same value of P(LOM). The CCDF is then constructed by integrating the pdf from right to left, i.e., in the direction of goodness for X_PM2. If the direction of goodness were left to right, then a CDF would be appropriate, rather than a CCDF.
- Risk tolerances for individual risk scenarios have been established for the performance markers defined for performance measure X_PM2. They are IRTL-G and IRTL-R for PMK-G and PMK-R, respectively. The IRTL values are set at a fraction of the values given for aggregate risk in Table 4-IV, consistent with the process for deriving IRTLs from RTLs in Section 3.3.4 of Part 1 of this handbook.
- $CCDF_{X\_RS3}$ falls below IRTL-R at PMK-R, but above IRTL-G at PMK-G, giving individual risk scenario X_RS3 a risk classification of Yellow/"Marginal" using the individual risk scenario classification process in Section 3.3.5 of Part 1 of this handbook.

4.3.1.2 Analysis and Classification of Individual Risk Scenario X_RS4, Thrust Oscillation Damages the Surface Nuclear Fission Reactor

The risk statement for risk X_RS4 is:

> *Given that finite element models show an unexpected coupling between the launch vehicle thrust oscillation and the structural vibration modes of the integrated vehicle, there is a possibility of vibration-induced damage to the surface nuclear fission reactor during launch, thereby leading to inoperability of the delivered surface nuclear fission reactor, adversely impacting the surface nuclear fission reactor and the achievement of Objective X2, "Ensure that the probability of loss of mission from an accident does not exceed the minimum expectation."*

Figure 4-2 shows an RSD for risk X_RS4 that is integrated into the intended path of the baseline plan, consistent with Figure 5-6 of Part 1 of this handbook. The RSD of X_RS4 is similar in form to that of X_RS3 above, but includes a pivotal event (Payload Adapter Failure), resulting in more than one possible end state should individual risk scenario X_RS4 be realized.

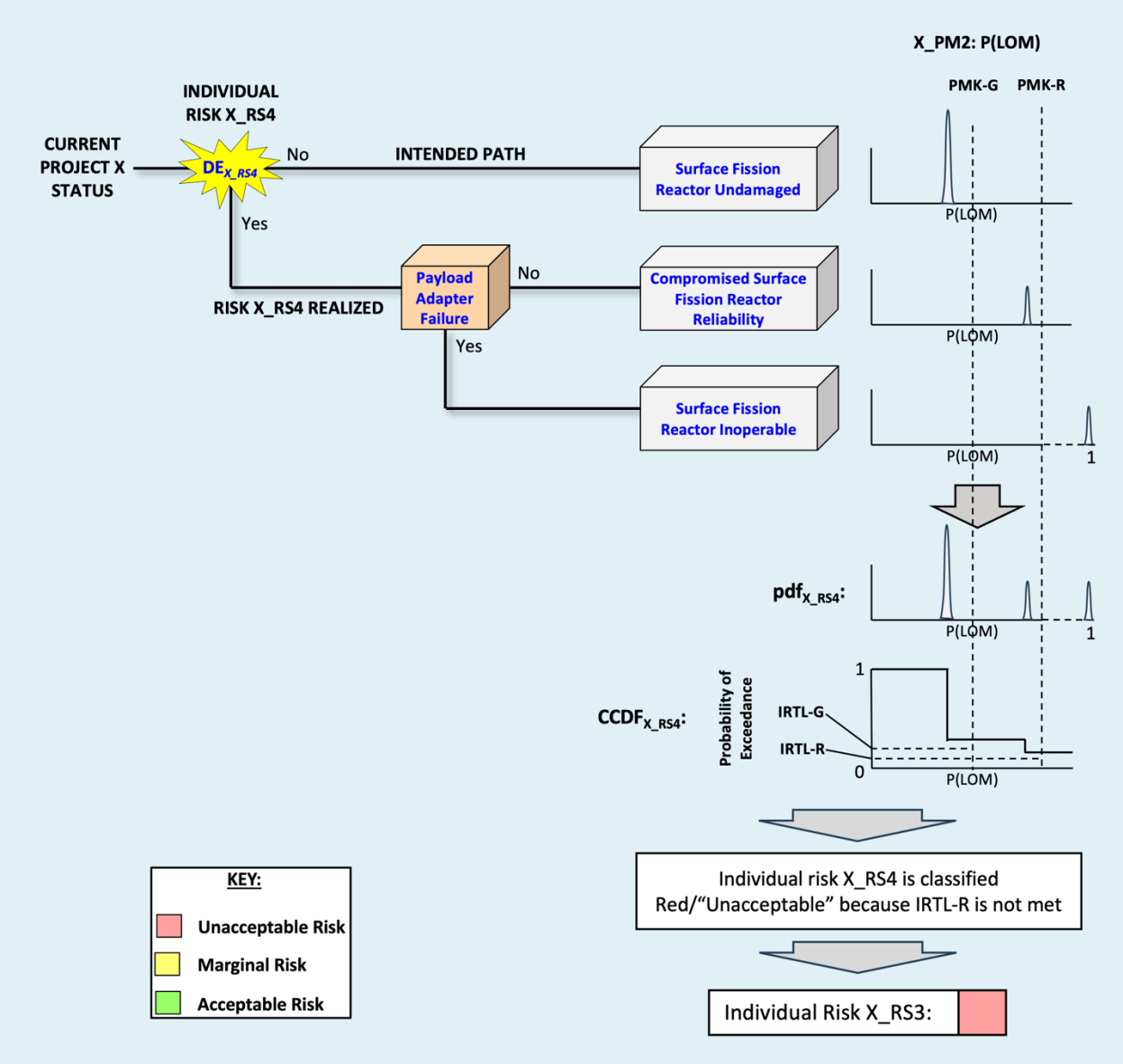


Figure 4-2. Probabilistic Analysis of Individual Risk Scenario X_RS4 (notional)

In Figure 4-2:

- The current project status includes the condition that motivated the identification of risk X_RS4, namely the coupling between the launch vehicle thrust oscillation and the structural vibration modes of the full-up vehicle.
- The departure event, DE_{X_RS4}, is vibration-induced damage to the surface nuclear fission reactor during launch. The probability of occurrence of DE_{X_RS4} would be based on vibrational analysis of the surface fission reactor, possibly supported by vibration testing (e.g., at sub-assembly level).
- The vibrational analysis (and possible testing) conducted as part of the analysis of X_RS4 indicates that the reactor would withstand the vibrational loads without outright failure, but

would likely result in reduced reliability over the required time in service. Fortunately, even with the reduced reliability, P(LOM) is still within the P(LOM) requirement, but it is not within the P(LOM) goal. The pdf for the end state, "Compromised Surface Reactor Reliability," captures the assessment of P(LOM) in the case where the reactor is damaged due to vibration during launch.

- However, the vibrational analysis also showed a probability of payload adapter failure, which if it occurred would result in an inoperable reactor and therefore mission failure. This is indicated by the pdf at P(LOM) = 1.
- $CCDF_{X\_RS4}$ exceeds IRTL-R at PMK-R giving individual risk scenario X_RS4 a risk classification of Red/"Unacceptable" using the individual risk scenario classification process in Section 3.3.5 of Part 1 of this handbook.

4.3.2 Heuristic Approach

In a heuristic approach, the likelihoods of the RSD end states, and the performance associated with each end state, are analyzed based on historical data, expert opinion, and engineering judgement. Risk matrices anchored to each affected top-level objective and associated risk tolerances are used as an intermediate step towards the classification of the individual risk scenario. In order to illustrate the differences between the probabilistic and heuristic approaches, the application of a heuristic approach to analyzing individual risk scenarios is illustrated using the same individual risk scenarios (i.e., risks X_RS3 and X_RS4) that were used to illustrate the probabilistic approach. Additionally, to provide an example of the heuristic approach in an institutional context, the heuristic approach is also applied to Center "Y" risk Y_RS2, *Increasing unavailability of Center "Y" test facility due to facility aging*.

4.3.2.1 Analysis and Classification of Individual Risk Scenario X_RS3, The In-Space LOX/Methane Engine is Not Matured to its Target Reliability

As with the probabilistic approach, the heuristic approach to analyzing individual risk scenario X_RS3 begins with the RSD, as shown in Figure 4-3.

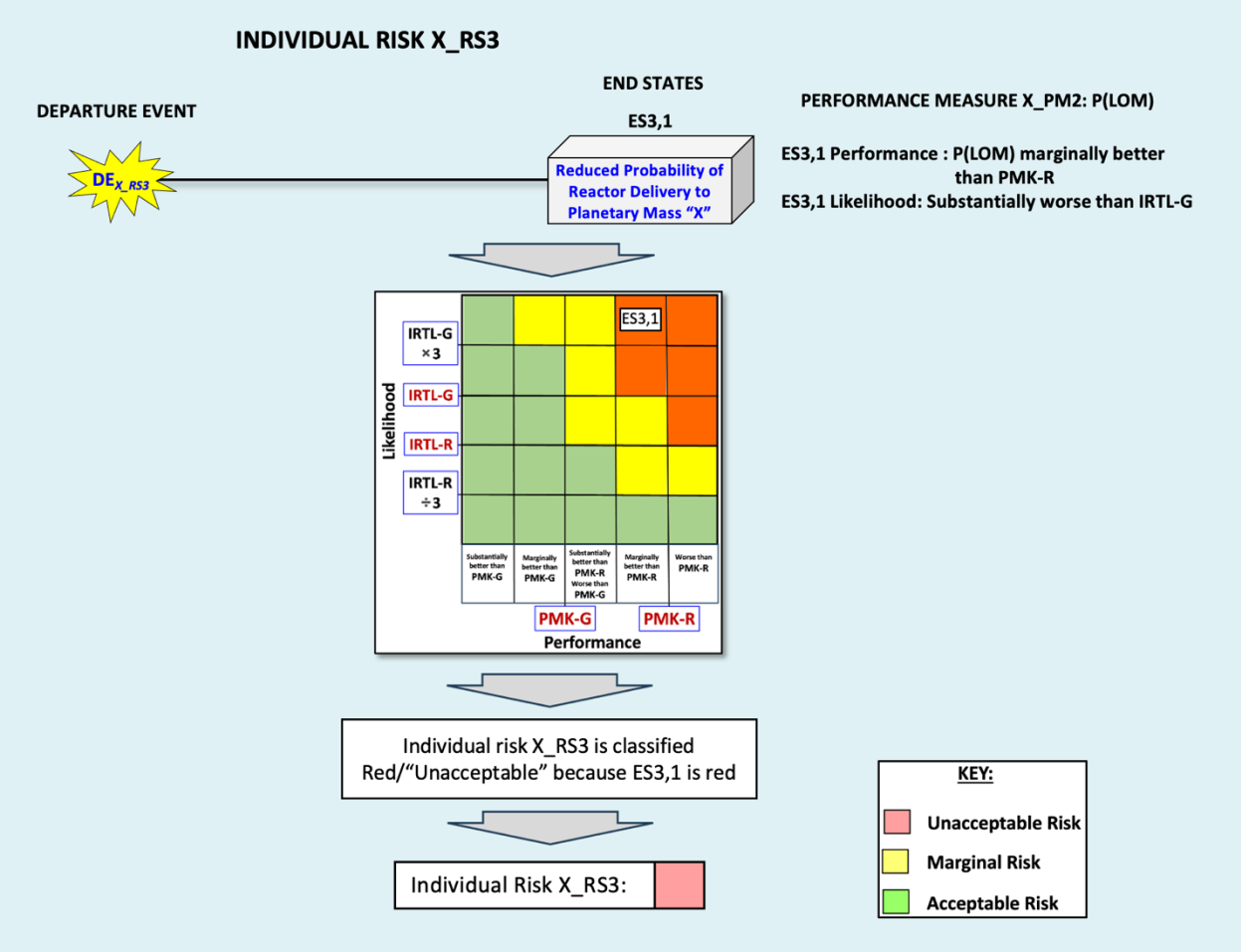


Figure 4-3. Heuristic Analysis of Individual Risk Scenario X_RS3 (notional)

The heuristic analysis of the RSD is illustrated to the right of the RSD in the figure. The classification of the individual risk scenario is illustrated below the RSD. Overall:

- The departure event, failure to achieve the target LOX/methane engine ignition reliability (DE_{X_RS3}), will occur if Project "X" cannot mature the LOX/methane engine to the point where it meets engine reliability specifications. The likelihood of DE_{X_RS3} is evaluated based on the expert judgement of the propulsion engineers and their assessment of the magnitude of the challenge presented by the combustion instability issue. Elicitation of such information would be facilitated by the project risk analysts. In this example, the likelihood of DE_{X_RS3} is assessed as relatively high, which, when expressed in terms of the established risk tolerance levels, is "Substantially worse than IRTL-G."
- If the LOX/methane engine cannot be matured to meet its reliability specifications, then the probability of mission failure increases with the increase in propulsion failure due to the unanticipated combustion instability. Given the vacuum test results, the propulsion subject matter experts (SMEs) conclude that Project "X" would not meet the P(LOM) performance goal, PMK-G, but would still very likely meet the P(LOM) performance

requirement, PMK-R. The reduced probability of reactor delivery to Planetary Mass "X" is therefore expressed as "Marginally better than PMK-R."

- With the heuristic analysis of individual risk scenario X_RS3 completed, the end states can be mapped to the risk matrix first discussed in Section 3.3.6 of Part 1 of this handbook. This is illustrated in Figure 4-3, where the end state where X_RS3 is realized is labeled "ES3,1" in accordance with a [risk #, end state #] convention. (In this case there is only one end state.)
- The risk classification of X_RS3 is determined using the procedure outlined in Section 3.3.6 of Part 1 of this handbook. Specifically, X_RS3 is classified as Red/ "Unacceptable" due to ES3,1 being in a red region of the risk matrix.

The heuristic and probabilistic approaches to individual risk scenario analysis and classification are not guaranteed to result in the same classification. In the current example of individual risk scenario X_RS3, the heuristic approach resulted in a Red/"Unacceptable" classification, whereas the probabilistic approach resulted in a Yellow/"Marginal" classification. Such differences are to be expected, considering that:

- The two approaches use different analysis methods, and the more qualitative or semi-quantitative analysis of the heuristic approach will likely involve relatively larger conservatisms to counter the possibility of underestimating the risk.
- The coloring of the risk matrix also imposes a degree of conservatism on risk classification to counter the possibility of underestimating the risk. In the case of X_RS3, ES3,1 maps to a red matrix element despite the performance being (marginally) better than PMK-R.

4.3.2.2 Analysis and Classification of Individual Risk Scenario X_RS4, Thrust Oscillation Damages the Surface Nuclear Fission Reactor

The analysis of individual risk scenario X_RS4 begins with the RSD shown in Figure 4-4.

As with risk X_RS3, the heuristic analysis of X_RS4 is illustrated to the right of the RSD in the figure and classification of X_RS4 is illustrated below the RSD. Overall:

- The likelihood of the departure event, vibration-induced damage to the surface nuclear fission reactor during launch (DE_{X_RS4}), is assessed by the relevant SMEs as close to IRTL-G × 3 based on vibrational analysis and testing, with a roughly fifty percent chance of payload adapter failure given vibration-induced damage to the reactor. This places both end states (ES4,1 and ES4,2) between IRTL-G and IRTL-G × 3 on the risk matrix.
- For end state ES4,1, the value of performance measure X_PM2 (i.e., P(LOM)) is assessed to be marginally within the P(LOM) requirement. P(LOM) for end state ES4,2 is unity due to the severe damage caused by payload adapter failure.
- With the heuristic analysis of individual risk scenario X_RS4 completed and mapped to the risk matrix, X_RS4 is classified as Red/ "Unacceptable" due both to ES4,1 being in a red region of the risk matrix and to ES4,2 being in a red region of the risk matrix. Either end state being in the red is enough to classify X_RS4 as Red/ "Unacceptable."

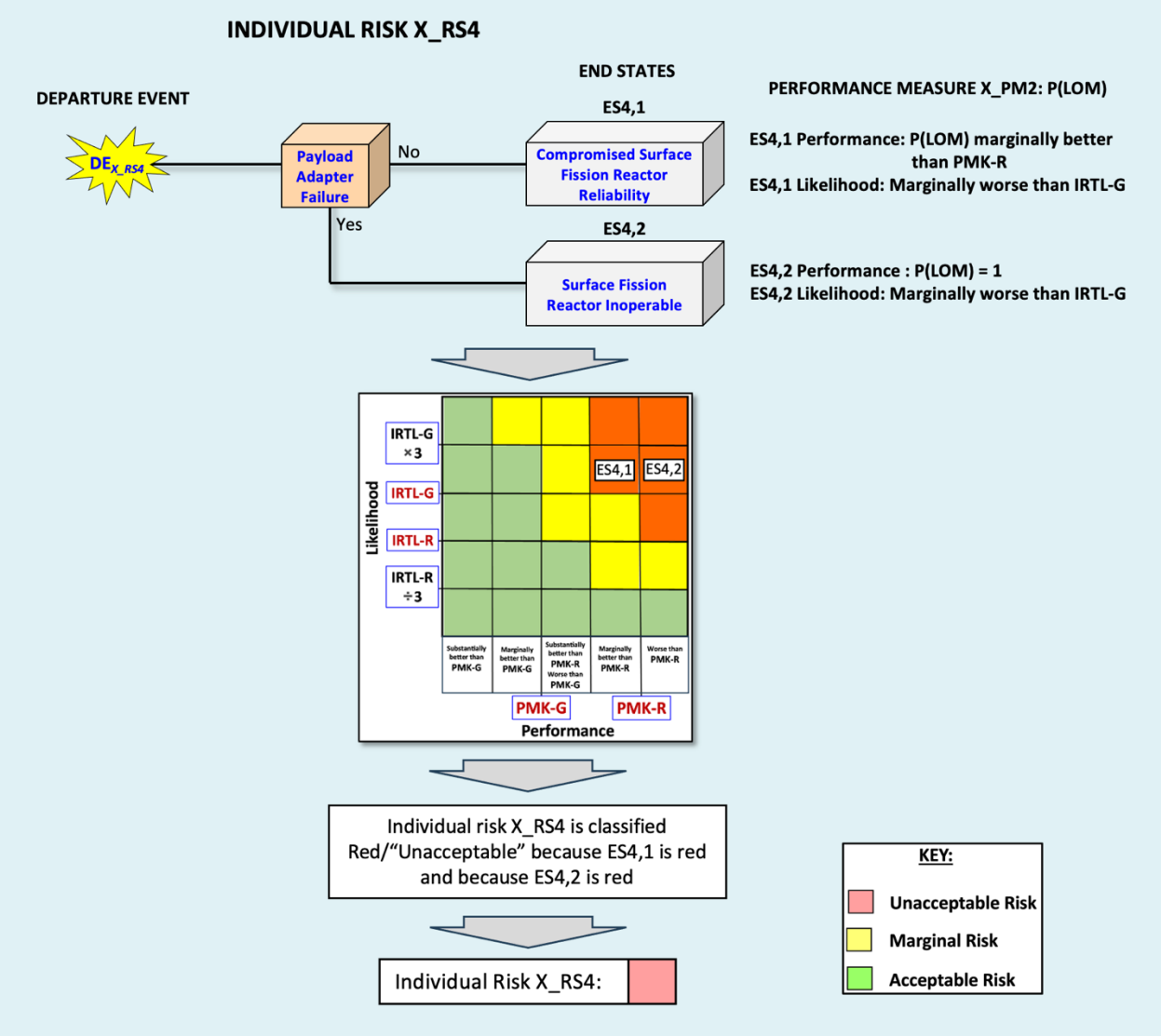


Figure 4-4. Heuristic Analysis of Individual Risk Scenario X_RS4 (Notional)

4.3.2.3 Analysis and Classification of Individual Risk Scenario Y_RS2, Increasing unavailability of Center "Y" test facility due to facility aging

The risk statement for risk Y_RS2 is:

> *Given the increasing rate of Center "Y" test facility component failures and increasing repair downtimes due to facility aging, there is a possibility that the test facility unavailability will exceed acceptable limits, thereby leading to delays in developing the Project "X" technologies that are dependent on Center "Y" testing for maturation, affecting Project "X" cost and schedule objectives, adversely impacting Project "X" success and the achievement of Objective Y2, "Ensure sufficient test facility availability to satisfy the needs of the Planetary Mass "X" surface nuclear reactor placement project."*

Figure 4-5 shows an RSD for risk Y_RS2.

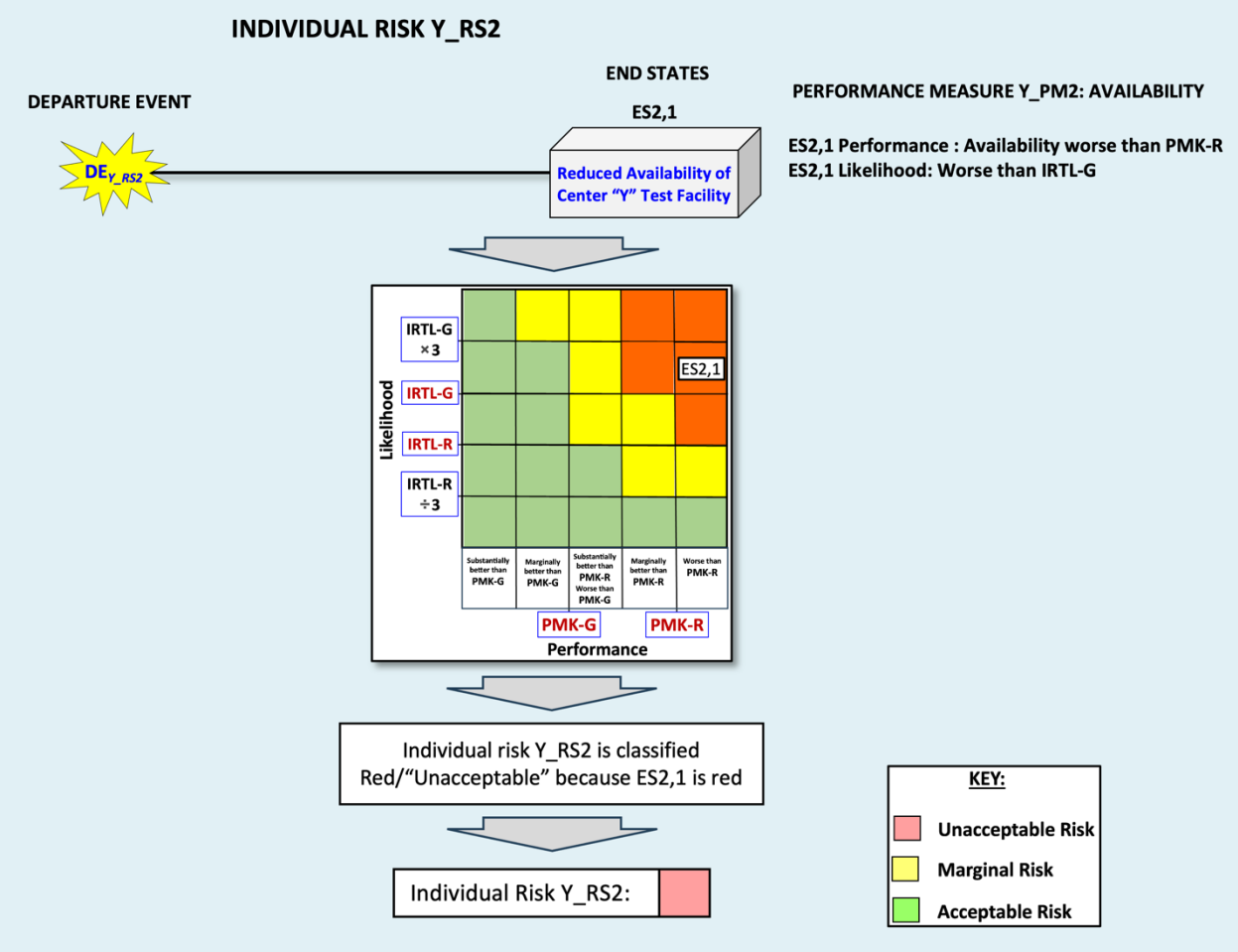


Figure 4-5. Heuristic Analysis of Individual Risk Scenario Y_RS2 (notional)

The heuristic analysis of the RSD is illustrated to the right of the RSD in the figure. The classification of the individual risk scenario is illustrated below the RSD. Overall:

- The departure event, test facility unavailability exceeding acceptable limits (DE_{Y_RS2}), will eventually occur due to facility aging. The likelihood that test facility availability will fall below the 80% PMK-R value during the period of time where it is needed for Project "X" is assessed as being over 10%, based on the history of failures and repair times at the facility, estimates for the times to repair the specific components considered most likely to fail, and projections of facility component unreliability, based on surveillances, analyses, and expert judgement.
- Risk tolerances for individual risk scenarios have been established for the performance markers defined for performance measure Y_PM2. They are IRTL-G and IRTL-R for PMK-G and PMK-R, respectively. The IRTL values are set at a fraction of the values given for aggregate risk in Table 4-V, consistent with the process for deriving IRTLs from RTLs in Section 3.3.4 of Part 1 of this handbook.

- This “semi-quantitative” analysis conducted on Y_RS2 is sufficient to place its (single) end state, ES2,1, into a red risk matrix element, as shown in Figure 4-5. This in turn is sufficient to classify individual risk Y_RS2 as Red/”Unacceptable.”

4.4 Probabilistic and Heuristic Approaches for Analyzing Aggregate Risks

Probabilistic and heuristic approaches to risk aggregation are illustrated in this section, using the objective X2 and the individual risk scenarios X_RS3 and X_RS4. As discussed in Section 4.3, probabilistic approaches are preferred where practicable.

4.4.1 Probabilistic Approach

Various sections of Chapters 3 through 5 in Part 1 discuss the fundamentals of the probabilistic analysis approach, which is characterized by the development of RSDs for individual risk scenarios and the aggregation of those risks within an integrated risk model. Figure 4-6 illustrates the calculation and classification of aggregate risk, leveraging the analyses of individual risk scenarios illustrated in Section 4.3.1 above. The procedure is discussed generically in Section 3.2.6 of Part 1 of this handbook. Figure 4-6 below is an instantiation of Figure 3-8 in that section. For simplicity, Unknown and/or Underappreciated (U/U) risk has been neglected in this example.

Like Figure 4-1 and Figure 4-2, Figure 4-6 shows risk scenarios that are departures from the nominal intended path of Project “X”. In the case of the integrated risk model, however, the branches of the diagram include all possible combinations of individual risk scenario realizations. Depending on the nature and timing of the individual risk scenarios, the set of possible combinations can become large, and the likelihoods and consequences of an individual risk scenario can be conditioned by the occurrence of prior risk realizations. These issues are addressed in [3].

In the case of individual risk scenarios X_RS3 and X_RS4, the y probabilities of occurrence are independent of each other, so they can be placed in a simple sequence. Figure 4-6 puts X_RS3 first in the sequence because its realization, if it occurs, is during LOX/methane engine development. Individual risk scenario X_RS4 is second, since its realization, if it occurs, is during launch. From there, the mechanics of the process are essentially the same as for the individual risk scenarios separately, resulting in the illustrated pdf and CCDF for performance with respect to X_PM2: P(LOM).

Given the CCDF for P(LOM), the risk to objective X2, “*Ensure that the probability of loss of mission from an accident does not exceed the minimum expectation*,” can be classified using the risk tolerance levels for aggregate risk (i.e., RTL-G and RTL-R) that are specified in Table 4-IV, and the risk classification scheme of Table 3-I in Section 3.3.2 of Part 1 of this handbook. Because RTL-G is not met, the risk to objective X2 is Yellow/“Marginal.” This might at first seem to be at odds with the risk classification of individual risk scenario X_RS4 as Red/“Unacceptable,” but this illustration includes only two individual risk scenarios, whereas the derivation of IRTLs from RTLs typically assumes upwards of 10, as discussed in Section 3.3.4.3 of Part 1. In other words, these two individual risk scenarios are worrisome in the context of the full set of individual risk scenarios that are expected to be identified for Project “X”, but together on their own do not violate the P(LOM) risk tolerance levels.

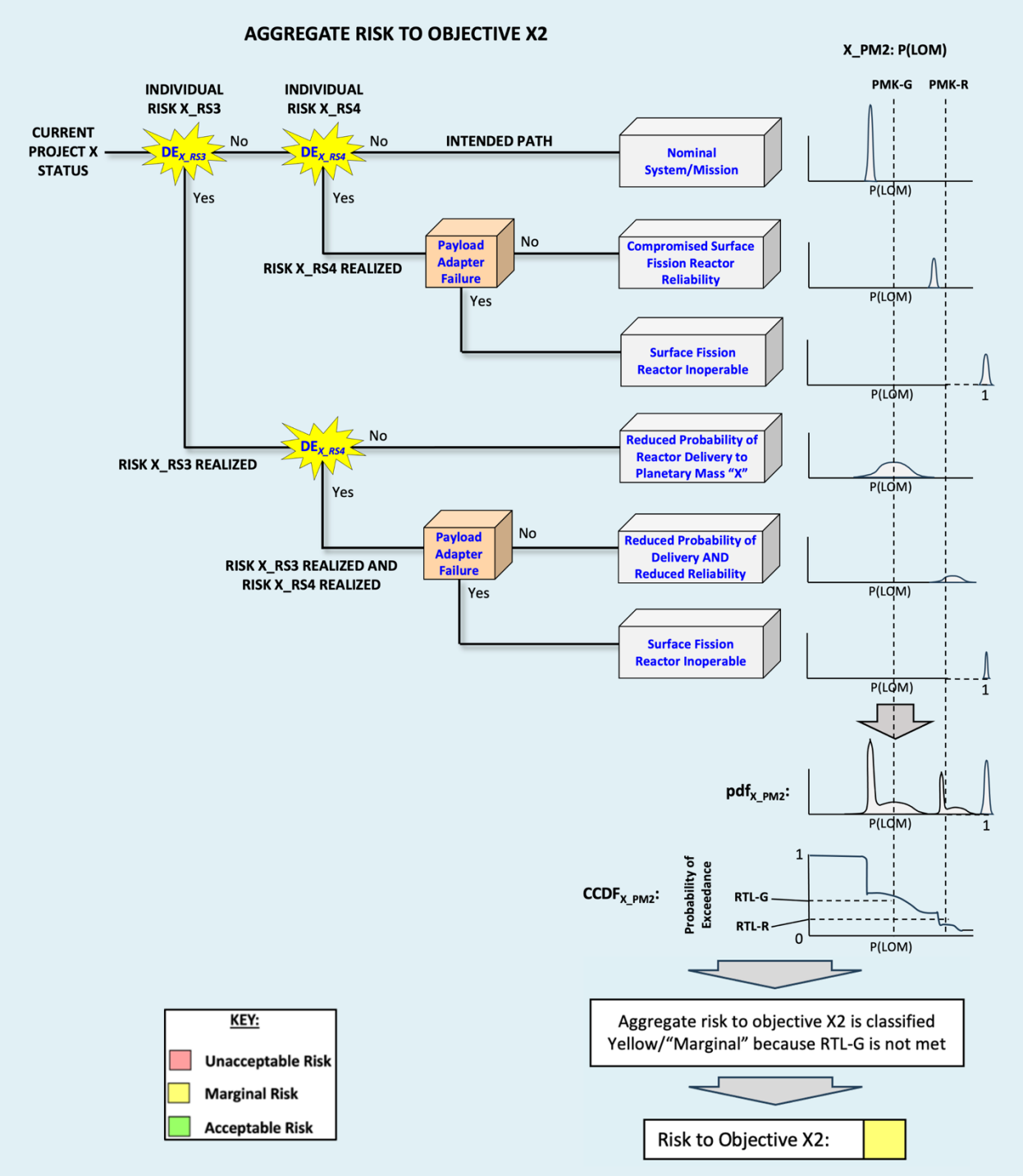


Figure 4-6. Probabilistic Analysis of Aggregate Risk to Objective X2 (notional)

The integrated risk model of Figure 4-6 is prior to the implementation of any risk controls for individual risk scenarios X_RS3 and X_RS4. As such, it can serve as the basis for developing risk models in support of Activity-Execution RIDM. Each alternative analyzed during Activity-Execution could be represented in an alternative-specific integrated risk model that accounts for the preventive and mitigative features under consideration. This would be reflected in the model

by new branches, the modification of existing event likelihoods, the elimination of branches rendered moot by the controls, and/or the transformation of end state consequences. Additional supporting models and/or analyses could be leveraged or developed.

4.4.1.1 *Accounting for Unknown and/or Underappreciated (U/U) Risk Scenarios Alongside the Probabilistic Approach*

As discussed in Part 1 Section 3.2.2, quantitative logic models used in the probabilistic approach work with and rely upon identified risk scenarios and analyze their progression from initiating events to end states; however, such logic models are inherently subject to incompleteness because of the inevitable existence of scenarios that are unknown and/or underappreciated. Accounting for the potential effects of U/U scenarios on performance measure output distributions requires knowledge of past history; particularly, consideration of the difference between the magnitudes of the performance measures that been observed in practice and those that are calculated using best estimate models. As discussed in Part 1 Section 4.7.3.4, and Appendix H, these difference are often best expressed in terms of a ratio: i.e., the magnitude of the performance measure of interest actually observed divided by the magnitude predicted by the models. For example, if for a particular program or project completed prior to the start of Project "X" was predicted to have a cost of between $0.75 billion and $1 billion, but in fact had a cost of $3 billion, the ratio of actual cost to predicted cost could be inferred to be between 3 and 4. The magnitude of cost attributable to U/U risk scenarios would correspondingly be between 2 and 3 times the magnitude of cost attributable to known scenarios. Typically, such a difference would be characteristic of a rather extreme case involving a landmark undertaking that had never been attempted before.

Part 1 Appendix B presented a set of leading indicators that typically correlate with the magnitude of the ratio of actual to predicted values for the performance measures of interest. They included diverse factors such as design or implementation complexity, use of new technology, stressful time pressures, and failure to employ good management practices. In Section 3.2.4 of Part 1, an example correlation was presented showing a strong relationship between actual program cost and design complexity over a large number of missions (see Figure 3-6 of that section). In these cases, the correlations made use of data from a large, diverse set of programs and projects.

For programs and projects conducted by NASA that are considered critical and that either utilize new, cutting-edge technology or apply existing technology in a new way, it is necessary to draw inferences from these correlations about the potential effects of U/U risks. The project manager for Project "X" accordingly includes such analysis in the RM plan.

4.4.2 Heuristic Approach

This section illustrates a heuristic approach for determining performance measure risks. Figure 4-7 illustrates the process, leveraging the analyses of individual risk scenarios illustrated in Section 4.3.2 above. The procedure is discussed generically in Section 5.3.3.3 of Part 1 of this handbook. Figure 4-7 is an instantiation of Figure 5-14 in that section.

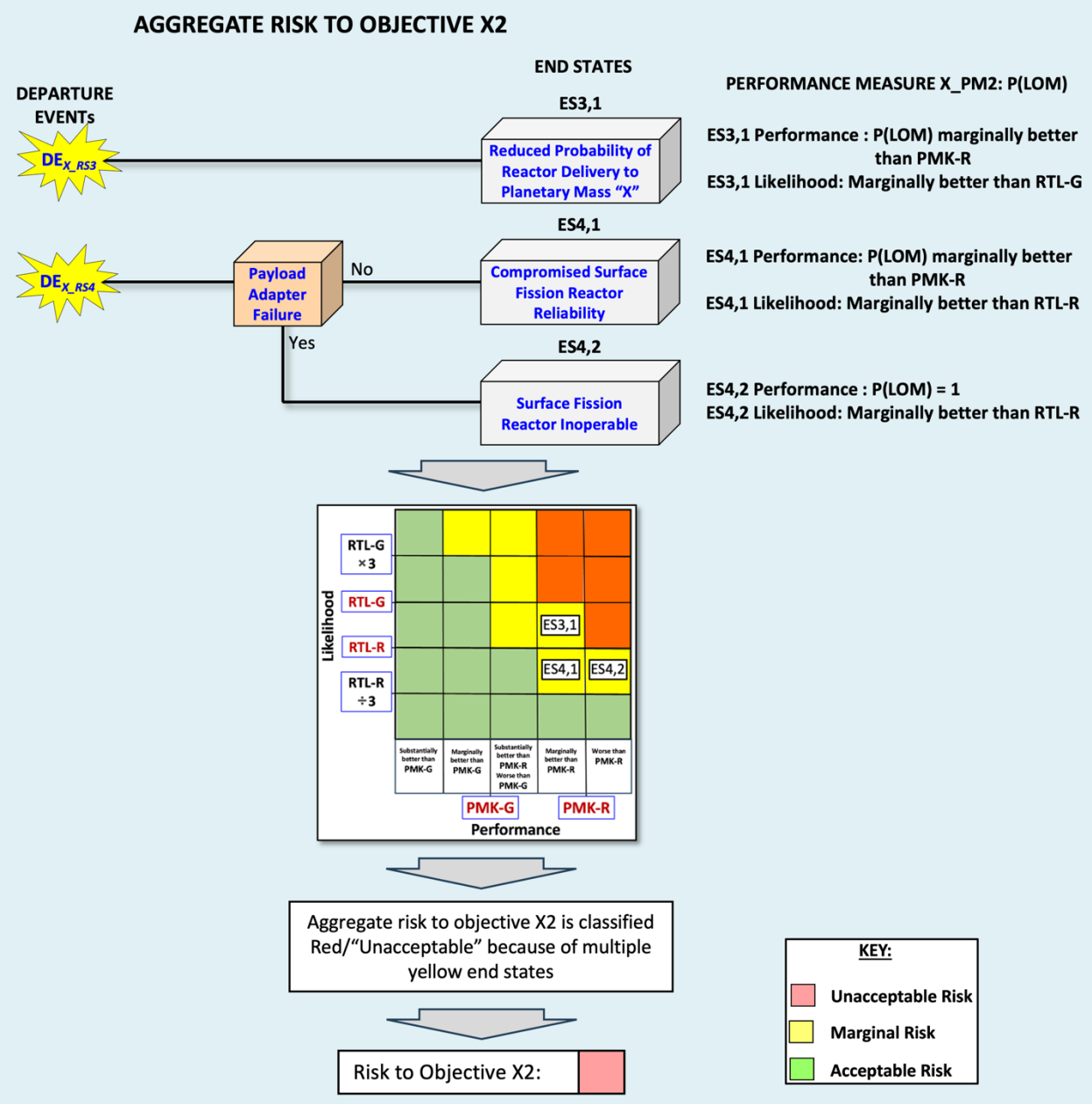


Figure 4-7. Heuristic Analysis of Aggregate Risk to Objective X2 (notional)

The heuristic analysis of aggregate risk begins with the same RSDs and end state likelihoods and performance measure values that were developed to analyze individual risk scenarios, as illustrated in Figure 4-3 and Figure 4-4. Then the end states for every individual risk scenario affecting the objective in question are mapped to the risk matrix for aggregate risk that was developed for that objective. (This is the matrix that has RTL-R and RTL-G on the y-axis, rather than IRTL-R and IRTL-G.) In the illustrated case of objective X2 and individual risk scenarios X_RS3 and X_RS4 there are three end states: ES3,1, ES4,1 and ES4,2.

Once the end states have been mapped to the matrix, the risk classification procedure is executed to determine the overall risk classification. In the example, the operative rule is:

- If there are multiple Yellow/"Marginal" mappings in a matrix, then the individual risk scenario is classified as Red/"Unacceptable" with respect to the objective unless a defensible argument can be made that the cumulative effect of the multiple Yellow/"Marginal" paths is still Yellow/"Marginal."

In the case of the three end states shown in Figure 4-7, an argument cannot be made that the cumulative effect of the three yellow end states is still yellow. On the contrary, the SMEs are able to make a positive argument that the cumulative effect of the end states is red. They agree that the likelihood of one or another of the three end states occurring is greater than RTL-G, given that the likelihood of ES3,1 on its own is only marginally less than RTL-G. Furthermore, they reason that if the performance of ES4,2 with respect to X_PM2 were "marginally better than PMK-R" instead of "worse than PMK-R" (i.e., if all three end states were in the same performance bin on the matrix), the cumulative rating would be red because that situation could be represented by a single end state in the second row of the fourth column of the matrix, which is red. In other words, the SMEs reason that even if the risk profile were better than it actually is, objective X2 would still be red. Therefore, the risk to objective X2 is classified as Red/"Unacceptable."

As was the case for the analysis of individual risk scenario X_RS3 in Section 4.3.2.1, the probabilistic and heuristic approaches to analyzing aggregate risk yield different results for the risk classification of objective X2. The reasons here are the same as the reasons given in that section, namely:

- The two approaches use different analysis methods, and the more qualitative or semi-quantitative analysis of the heuristic approach will likely involve relatively larger conservatisms to counter the possibility of underestimating the risk. In fact, the analysis of aggregate risk leverages the analyses of individual risk scenarios, so any conservatisms introduced there are carried forward into the aggregate analysis.
- The coloring of the risk matrix also imposes a degree of conservatism on risk classification to counter the possibility of underestimating the risk. In the case of objective X2, the argument for the Red/"Unacceptable" risk classification was largely driven by the red coloring of the matrix element in row two, column four, which has a performance that is (marginally) better than PMK-R.

4.5 Activity-Execution RIDM

As illustrated by Figure 5-18 in Part 1 of the handbook, Activity-Execution RIDM is conducted during CRM *Plan* as the process for developing risk responses when a level of rigor and formality is needed to adequately identify risk response options, assess their potential effectiveness, and document the rationale for selecting the implemented response. Examples of Activity-Execution RIDM are illustrated here. As discussed in Section 4.3, where practicable, probabilistic approaches are preferred over heuristic approaches; however, in some contexts heuristic approaches may be necessary and/or appropriate.

The following sections illustrate both the probabilistic approach as well as the heuristic approach. The probabilistic approach is used to illustrate Activity-Execution RIDM for a programmatic risk. The heuristic approach is used to illustrate Activity-Execution RIDM for an institutional risk.

4.5.1 Illustration of a Probabilistic Approach to Activity-Execution RIDM

The individual risk scenario used for illustrating a probabilistic approach to Activity-Execution RIDM is X_RS3:

> *Given that prototype LOX/methane engine vacuum start tests indicate the presence of unanticipated combustion instability, there is a possibility that the target LOX/methane engine ignition reliability is not achieved, thereby leading to decreased probability of successfully delivering the reactor to the surface of Planetary Mass "X", adversely impacting LOX/methane engine and the achievement of Objective X2, "Ensure that the probability of loss of mission from an accident does not exceed the minimum expectation."*

The risk response trade space should be as comprehensive as practicable, in order to optimize the resulting activity performance at acceptable levels of risk. Ideally, the risk response should be holistic, accounting for all sources of risk within the integrated risk model of the activity. However, in practice, where individual risk scenarios are often identified and managed one at a time, it can be the case that the management of a given individual risk scenario is conducted in relative isolation from the management of other open individual risk scenarios. This is especially true when the underlying risk drivers are localized and independent from one another.

In the case of risk X_RS3, combustion instability is considered a local phenomenon, so Project "X" decides to develop a risk response using the risk model of the individual risk scenario (as illustrated in Figure 4-1) rather than the integrated risk model (as illustrated in Figure 4-6). After developing and down-selecting from a broad set of possible responses, Project "X" settles on two contending alternatives (in addition to the no-action alternative):

1. Increase funding to the LOX/methane engine development activity, enabling multiple combustion instability control strategies to be pursued in parallel, such as the design and testing of injector face baffles and acoustic absorbers. The propulsion SMEs are cautiously optimistic that the combustion instability can be resolved given the time and resources needed to find a successful engineering solution. If successful, this alternative also has the virtue of producing a reliable LOX/methane engine for use in other programs.
2. Abandon the LOX/methane engine development activity and switch to a monomethylhydrazine/nitrogen tetroxide engine for TLM propulsion. This would be a mature solution with a high technology readiness level (TRL) and a high engine start reliability. However, the specific impulse of the monomethylhydrazine/nitrogen tetroxide engine is lower than that of the LOX/methane engine, necessitating a correspondingly larger TLM. The down-select process weeded out monomethylhydrazine/nitrogen tetroxide solutions requiring redesign of other stages, but a substantially new TLM would be needed, along with a recalibrated mission profile to account for the more massive stage and longer burn duration.

4.5.1.1 Risk Analysis of Alternative 1, Accelerated Combustion Instability Prevention

Figure 4-8 illustrates the risk analysis of Alternative1, *Accelerated Combustion Instability Prevention*.

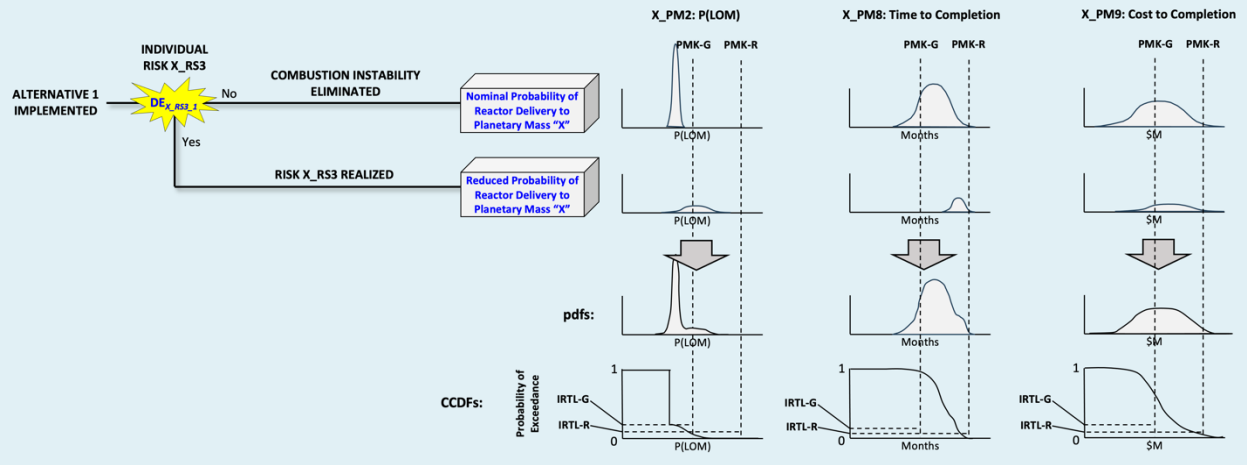


Figure 4-8. Risk Analysis of Alternative1, Accelerated Combustion Instability Prevention

In Figure 4-8:

- Although individual risk scenario X_RS3 was assessed in Figure 4-1 as affecting only performance measure X_PM2, *P(LOM)*, Alternative 1 would take time to implement and would incur additional project costs, so its analysis must address the impact of the additional cost and schedule burdens on the performance measures X_PM8, *Time to Completion*, and X_PM9, *Cost to Completion*.
- Although Alternative 1 is analyzed as bringing the X_PM2 risk down to Green/ "Acceptable," the impact on cost and schedule is significant, resulting in Yellow/ "Marginal" classifications for both X_PM8 and X_PM9, since neither are within their respective IRTL-G values.

4.5.1.2 Risk Analysis of Alternative 2, Monomethylhydrazine/Nitrogen Tetroxide Engine

Figure 4-9 illustrates the risk analysis of Alternative 2, *Monomethylhydrazine/Nitrogen Tetroxide Engine*.

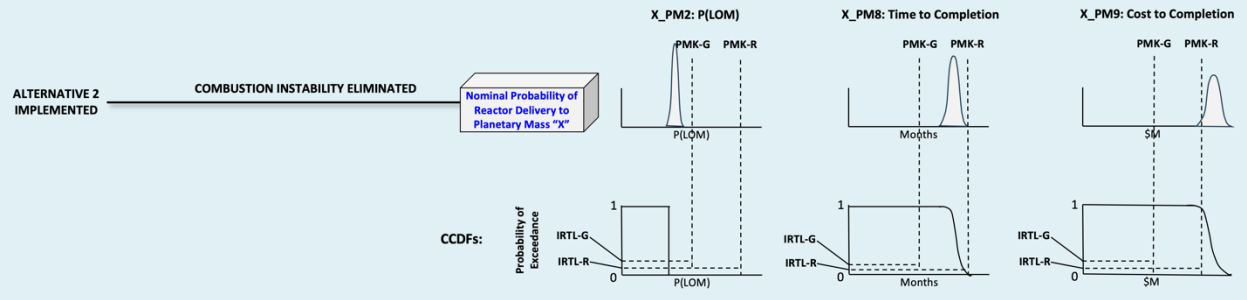


Figure 4-9. Risk Analysis of Alternative 2, Monomethylhydrazine/Nitrogen Tetroxide Engine

In Figure 4-9:

- Alternative 2 eliminates the source of individual risk scenario X_RS3 by removing the LOX/methane engine from the TLM and replacing it with a high-TRL monomethylhydrazine/nitrogen tetroxide engine. As a result, the only path in the RSD of Figure 4-9 is the nominal path for the modified system.

- Because the replacement engine is a mature technology, the cost and schedule impacts are relatively well known, resulting in fairly narrow pdfs.
- The effect of Alternative 2 on cost and schedule risk is significant. The risk to X_PM8, *Time to Completion*, is Yellow/"Marginal," and the risk to X_PM9, *Cost to Completion*, is Red/"Unacceptable."

4.5.1.3 Risk Analysis of the "No Action" Alternative

Keeping in mind that "ACCEPT" is a valid NPR 8000.4 risk disposition, Figure 4-10 illustrates the risk analysis of the *No Action* alternative, expanding Figure 4-1 to include the performance measures brought into the trade space by the other alternatives. In the case of the *No Action* alternative, because risk X_RS3 does not affect X_PM8, *Time to Completion*, or X_PM9, *Cost to Completion*, these performance measures are set at their nominal mean values. Consequently, their pdfs are delta functions and their CCDFs are step functions. As discussed in Section 4.3.1.1, the risk to X_PM2 is classified as Yellow/"Marginal." The risks to X_PM8 and X_PM9 are both Green/"Acceptable," consistent with their baseline planning targets.

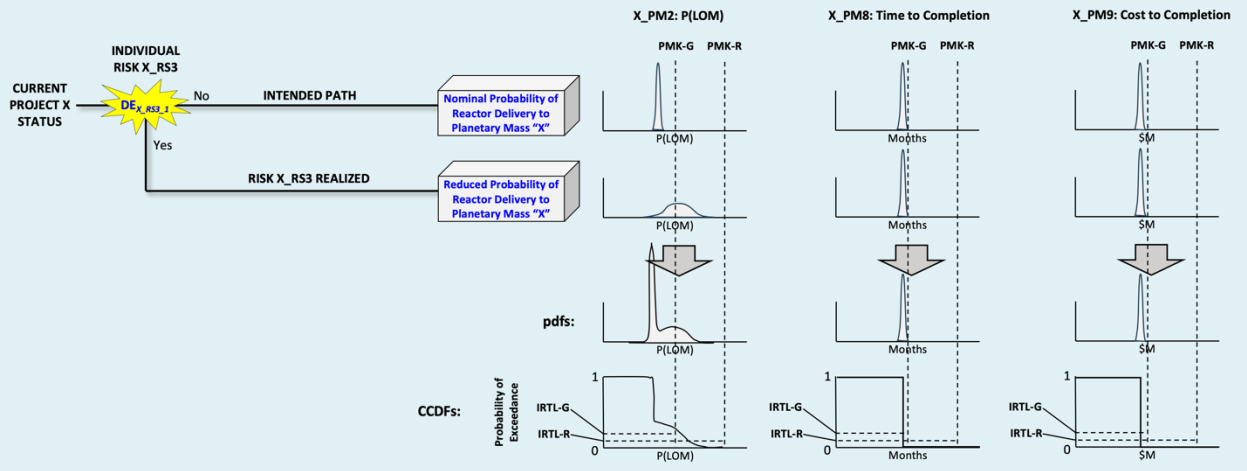


Figure 4-10. Risk Analysis of the No Action Alternative

4.5.1.4 Selection of a Risk Response to Risk X_PM3, The In-Space LOX/Methane Engine is Not Matured to its Target Reliability

Figure 4-11 presents a spider chart comparing the three risk response alternatives to individual risk scenario X_RS3. The chart shows the three affected performance measures explicitly, and consolidates the remaining unaffected performance measures into "Other PMs." Some noteworthy observations that can be quickly made from Figure 4-11 are:

- Both Alternative 1 and Alternative 2 successfully reduce the P(LOM) risk from X_RS3 to Green/"Acceptable," albeit at a cost to X_PM8 and X_PM9.
- No alternative is classified as Green/"Acceptable" across all performance measures. This means that Project "X" is not authorized to unilaterally implement a risk response without concurrence from the overseeing organizational entity, which in this case is the responsible Mission Directorate.

- Alternative 2 is dominated by Alternative 1, at least within the resolution of the risk categorization (R/Y/G). If the risk response decision were entirely risk-based, rather than risk-informed, this would suggest eliminating Alternative 2 from contention. However, because other factors may enter the deliberation, and because the overseeing organizational entity is necessarily involved in the decision (because there is no all-green alternative), Alternative 2 is retained as an option.

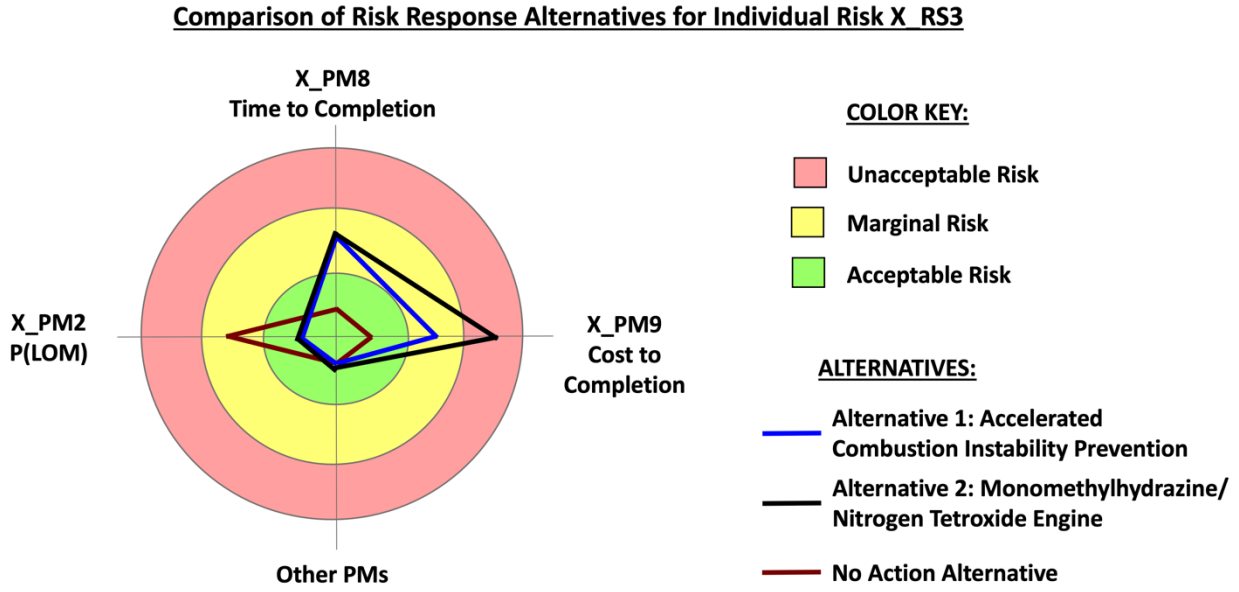


Figure 4-11. Comparison of Risk Response Alternatives for Individual Risk X_RS3

In this example, Project "X" recommends implementing Alternative 1, *Accelerated Combustion Instability Prevention*. That is the alternative that mitigates the risk to X_PM2 from X_RS3 to Green/"Acceptable" with the minimum risk impact to other performance measures. It also retains the LOX/methane engine development aspect of Project "X", which the manager believes will have wide-ranging and long-lasting collateral benefits to future NASA programs and projects. However, the overseeing Mission Directorate is concerned about the possibility of failed technology maturation and is attracted to the prospect of eliminating the risk entirely by switching to a monomethylhydrazine/nitrogen tetroxide engine for in-space propulsion. The Mission Directorate also has allocated enough funding to its management reserve to enable it to relax Project "X"'s *Cost to Completion* requirement.

Therefore, the Mission Directorate chooses to add funding to Project "X" and rebaseline its *Time to Completion* and *Cost to Completion* performance markers. Because Project "X" is up against a launch window constraint, the Mission Directorate maintains the *Time to Completion* requirement and risk tolerance level, but relaxes the *Time to Completion* goal and risk tolerance level so that the risk is green (with respect to *Time to Completion*) but the rebaselined goal will still act as an early warning of threats to the requirement if new schedule risks emerge. The Mission Directorate relaxes the *Cost to Completion* requirement and goal to be consistent with the rebaselined budget. It keeps the existing risk tolerance level on the requirement, but relaxes it on the goal, similar to the treatment of *Time to Completion*. Figure 4-12 illustrates the rebaselined Project "X" in terms

of its rebaselined baseline performance and the associated performance markers and individual risk scenario tolerance levels. Figure 4-12 does not represent risk analysis results. Instead, it represents the baseline performance in the absence of risk. It is the template that will be used going forward to analyze individual risk scenarios, much as the two individual risk scenarios in Figure 4-1 and Figure 4-2 were analyzed from the perspective of their effects on the previous Project "X" baseline.

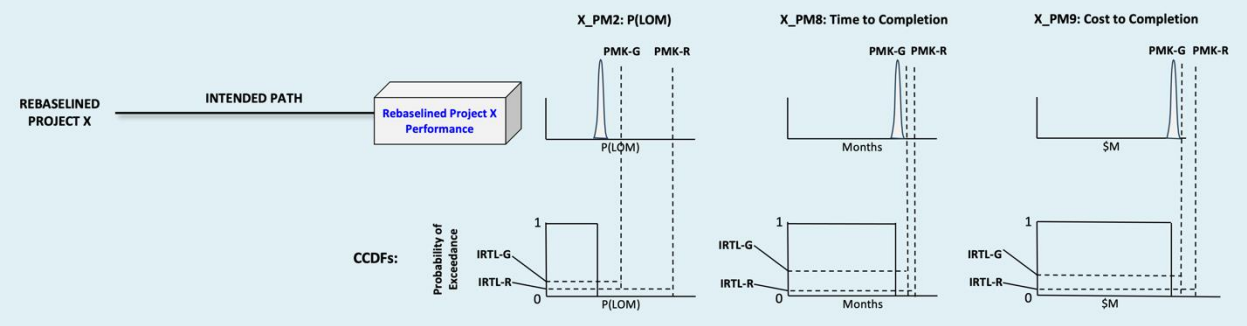


Figure 4-12. Rebaselined Project "X" After Responding to Risk X_RS3

4.5.2 Illustration of a Heuristic Approach to Activity-Execution RIDM

The individual risk scenario used for illustrating a heuristic approach to Activity-Execution RIDM is Y_RS2:

> *Given the increasing rate of Center "Y" test facility component failures and increasing repair downtimes due to facility aging, there is a possibility that the test facility unavailability will exceed acceptable limits, thereby leading to delays in developing the Project "X" technologies that are dependent on Center "Y" testing for maturation, affecting Project "X" cost and schedule objectives, adversely impacting Project "X" success and the achievement of Objective Y2, "Ensure sufficient test facility availability to satisfy the needs of the Planetary Mass "X" surface nuclear reactor placement project."*

Y_RS2 was analyzed in Section 4.3.2.3, where it was classified as Red/"Unacceptable."

4.5.2.1 Identification of Risk Response Alternatives

As with the example in Section 4.5.1, the risk response trade space should be as comprehensive as practicable. In the case of Y_RS2, two alternatives are initially identified by Center "Y" (in addition to the no-action alternative):

1. Refurbish the Center "Y" test facility as needed to ensure that the target availabilities listed in Table 4-V are within their corresponding risk tolerance levels. The philosophy behind this alternative is to manage the Project "X"-related unavailability risk at minimum cost. The alternative will require the test facility to be taken offline for the duration of the refurbishment, but once complete, the reliability of the facility's components will be high enough to ensure that the availability of the facility to Project "X" will be within the established risk posture for the remaining duration of the project's needs.
2. Construct a replacement Center "Y" test facility. The philosophy behind this alternative is to restore the reliability of Center "Y" test capabilities to an as-new condition in order to

effectively remove it as a source of risk not only to Project "X", but to all current and upcoming projects. This alternative will allow the existing facility to remain operational during construction, at which point the replacement test facility will take over and the old facility will be decommissioned and dismantled.

Additionally, given the prospect of constructing a replacement test facility, Center "Y" sees an opportunity to expand its test capabilities to better meet the spectrum of foreseeable future test needs and to more effectively attract talented scientists and engineers to the Center.[1] Therefore, Center "Y" identifies a third alternative:

3. Construct a modernized Center "Y" test facility. As discussed above, the philosophy behind this alternative is to reliably and effectively meet NASA's (and potentially other organizations') test needs into the foreseeable future, and to ensure Center "Y"'s continued status as a center of testing excellence.

4.5.2.2 Setting the Analysis Framework

Because this example is of Activity-Execution RIDM (as opposed to Activity-Planning RIDM), Center "Y"'s objectives, performance measures, performance markers, and risk tolerances are already established. Table 4-II lists the Center "Y" objectives and performance measures that are directly related to Project "X". Table 4-III lists Center "Y" objectives and performance measures related to cybersecurity. For this example, which is focused on Center "Y"'s test capabilities, the set of test-related objectives and associated performance measures in Table 4-IX are the ones that are relevant. They include objective Y2 from Table 4-II, as well as a number of objectives derived from NASA's Strategic Goal 4, *Enhance Capabilities and Operations to Catalyze Current and Future Mission Success* [4].

Table 4-IX. Objectives and Performance Measures for Risk Y_RS2 Response Planning

Objec. No.	Entity Objective	Perf. Meas. No.	Performance Measure
Y2	Ensure sufficient test facility availability to satisfy the needs of the Planetary Mass "X" surface nuclear reactor placement project	Y_PM2	Facility availability over the period of performance (% of time)
YY10	Meet the near-term testing needs of NASA and partner programs and projects	YY_PM10	Percent of testing needs met (%)
YY11	Meet the long-term testing needs of NASA and partner programs and projects	YY_PM11	Percent testing needs met (%)
YY12	Maintain Center "Y" as a center of excellence in testing	YY_PM12	Likert scale (1-5)
YY13	Stay within the budget allocated to the center for infrastructure development and maintenance	YY_PM13	Cost ($M)

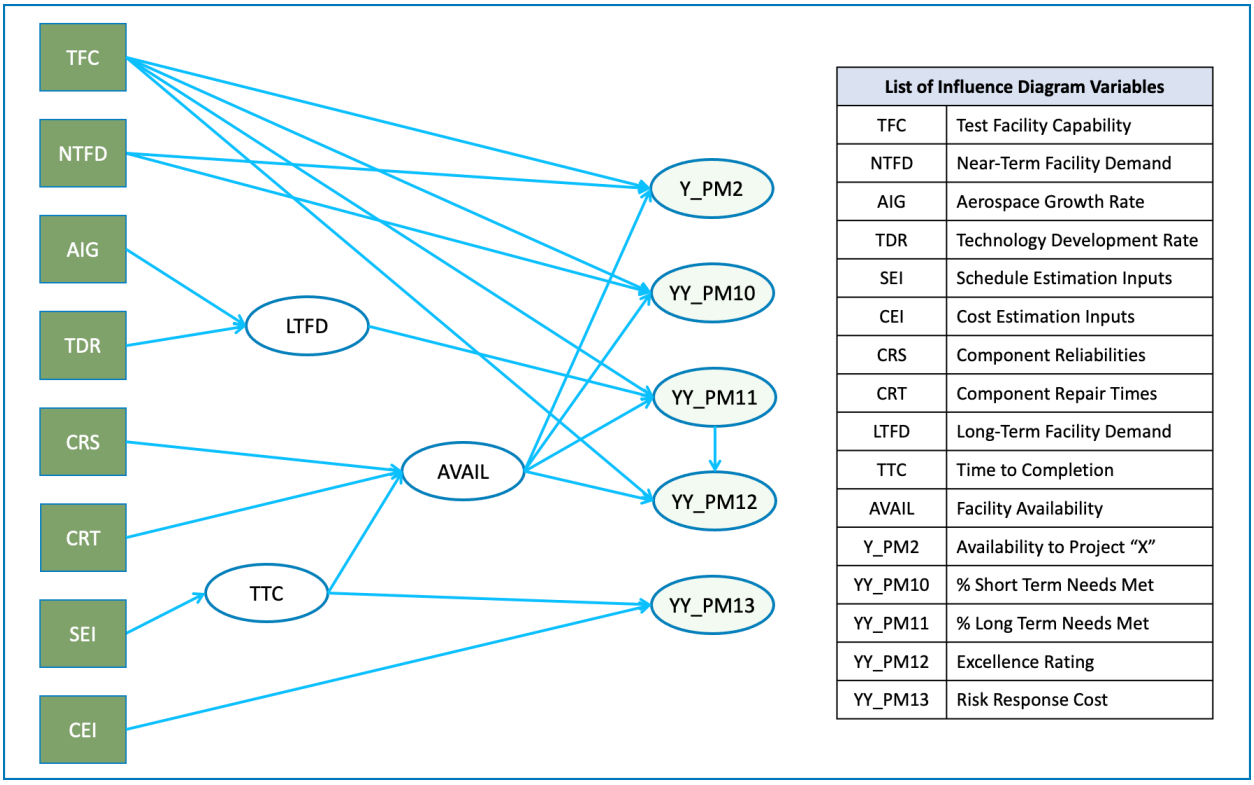
[1] Just as this example does not get into the specific nature of Center "Y"'s test facility capabilities, it also does not get into the nature of the proposed expanded capabilities. The expansion could be in the capacity that the facility can handle, or it could be in the types of tests that the facility can conduct, or both.

Table 4-X lists the performance markers and risk tolerances for the relevant objectives. Because they have been developed in an institutional management setting as opposed to an engineering management setting, they are not necessarily quantitative. Objective YY12 uses a Likert scale to measure the degree to which relevant stakeholders feel that Center "Y" is a center of excellence in testing. The corresponding risk tolerance levels are defined qualitatively, consistent with the subjective nature of the performance measure. Nevertheless, RTL-R for this objective is "Very Low," reflecting the high value of Center "Y"'s reputation as a center of excellence. Objective YY11 refers to the long term, about which there is high uncertainty, so although the performance markers are defined quantitatively, the risk tolerances are defined qualitatively to reflect the fact that projections of future capability relative to need are highly uncertain.

Table 4-X. Objectives, Performance Markers, and Risk Tolerance Levels for Risk Y_RS2 Response Planning

Objec. No.	Objective	PMK-G	PMK-R	RTL-G	RTL-R
Y2	Ensure sufficient test facility availability to satisfy the needs of the Planetary Mass "X" surface nuclear reactor placement project	90%	80%	10 %	5 %
YY10	Meet the near-term testing needs of NASA and partner programs and projects	90%	80%	30 %	15 %
YY11	Meet the long-term testing needs of NASA and partner programs and projects	90%	80%	Moderate	Low
YY12	Maintain Center "Y" as a center of excellence in testing	Likert: 5	Likert: 4	Low	Very Low
YY13	Stay within the budget allocated to the center for infrastructure development and maintenance	$50M	$60M	30 %	15 %

Once the relevant objectives have been identified along with their performance markers and risk tolerance levels, the next step in setting the analysis framework is to determine the factors upon which performance depends and trace them back to a set of quantifiable (or at least characterizable) input performance parameters (some of which may be uncertain). This process is discussed in general in Section 4.7 of Part 1 of this handbook. For the current example, Figure 4-13 illustrates one possible network of dependencies that could be used to analyze each alternative's performance measures. In this example, a single network is used to analyze each alternative. In general, however, if the alternatives are sufficiently different from one another, different parameters and dependencies might be used for the analysis of each alternative.



List of Influence Diagram Variables	
TFC	Test Facility Capability
NTFD	Near-Term Facility Demand
AIG	Aerospace Growth Rate
TDR	Technology Development Rate
SEI	Schedule Estimation Inputs
CEI	Cost Estimation Inputs
CRS	Component Reliabilities
CRT	Component Repair Times
LTFD	Long-Term Facility Demand
TTC	Time to Completion
AVAIL	Facility Availability
Y_PM2	Availability to Project "X"
YY_PM10	% Short Term Needs Met
YY_PM11	% Long Term Needs Met
YY_PM12	Excellence Rating
YY_PM13	Risk Response Cost

Figure 4-13. Influence Diagram of Factors of Relevance to Risk Y_RS2 Response Analysis

Figure 4-13 shows that for each of the four alternatives, the availability of the test facility to Project "X" (performance measure Y_PM2) depends on the availability of the test facility to conduct testing (AVAIL) (i.e., whether or not it's in service), the competition for facility resources from other users (NTFD), and the test capabilities of the facility itself (TFC). Closely related to this is the facility's ability to meet users' short-term test support needs (YY_PM10). The facility's ability to meet users' long-term needs (YY_PM11) is assessed similarly, except that it depends on estimates of long-term rather than near-term facility demand. The facility's rating as a center of testing excellence (YY_PM12) is assessed in terms of the facility's capabilities, its ability to meet users' long-term testing support needs (YY_PM11), and the overall availability of the test facility (on the grounds that a frequently out-of-service facility is antithetical to excellence). The cost of the risk response alternative depends on methodologically well-established cost estimating inputs (CEI) and the time to completion (TTC), which itself depends on methodologically well-established schedule estimation inputs (SEI). The availability of the facility to conduct testing (AVAIL) depends on the reliabilities and repair times of its components (CRS, CRT), along with (for the refurbish alternative) the time to complete the implementation of the risk response (during which the facility is off-line). (The non-refurbish alternatives do not entail taking the facility off-line during risk response implementation.) Finally, the long-term facility demand (LTFD) depends on estimates of the growth rate of the aerospace industry (AIG) along with the rate of aerospace technological development. Higher rates of either of these factors are expected to produce correspondingly higher demand for testing.

It is important to note that the dependencies shown in Figure 4-13 represent just one way to structure the analysis, and that other representations are possible. For example, Figure 4-13 does not show that the cost of each alternative depends on the capability being developed. In particular, the expanded capability of the *modernized test facility* alternative comes at a comparatively high cost, but that dependency isn't shown in Figure 4-13. Instead, it is understood by the analysts that each alternative is defined (in part) by its capability and its cost estimating inputs, and although these are correlated, they can be treated as separate individual inputs to the analysis.

Keeping in mind that risk analysis consists of performance assessment supported by probabilistic modeling (see Section 4.4.2 in Part 1 of this handbook), it is necessary to characterize the uncertainties in the analyzed performance measures. Practically, this involves characterizing the uncertainties in the input performance parameters, then propagating them through the analysis to produce uncertain performance measure values. Table 4-XI presents a discussion of the input performance parameter uncertainties for each of the risk response alternatives.

Table 4-XI. Performance Parameter Uncertainties as a Function of Risk Response Alternative

Performance Parameters	**Risk Response Alternatives**			
	No Action	**Refurbish**	**Replace**	**Modernize**
TFC	Existing capability. No uncertainty.			Expanded capability. No uncertainty.
NFTD	Known. Negligible uncertainty.			
AIG	Large uncertainty. Qualitatively/semi-quantitatively estimable from existing projections and the NASA Strategic Plan.			
TDR	Large uncertainty. Qualitatively/semi-quantitatively estimable from existing projections and the NASA Strategic Plan.			
CRS	Known. Negligible uncertainty.	New components will be highly reliable. Negligible uncertainty.		
CRT	Known. Negligible uncertainty.	New components will be highly reliable. Repair times will be negligible. Negligible uncertainty.		
SEI	N/A	Short duration implementation. Uncertainties per established estimation methodology.	Long duration implementation. Uncertainties per established estimation methodology.	Long duration implementation. Uncertainties per established estimation methodology.
CEI	N/A	Low cost. Uncertainties per established estimation methodology.	Moderately high cost. Uncertainties per established estimation methodology.	High cost. Uncertainties per established estimation methodology.

Table 4-XI shows that there are two types of uncertainty that bear upon the management of risk Y_RS2. There is cost and schedule uncertainty having to do with refurbishment and construction, for which well-established methods exist such as those in the NASA Cost Estimating Handbook [5]. These uncertainties affect performance parameters SEI and CEI. Then there is uncertainty associated with the future of the aerospace industry, the degree to which it will or will not grow,

and the rate of technological innovation within it. These uncertainties are challenging to characterize and are arguably speculative. They affect performance parameters AIG and TDR.

4.5.2.3 Analyzing the Risk Response Alternatives

The heuristic analysis illustrated in this section takes a minimalist approach to comparing the performance of each risk response alternative to the performance markers and risk tolerance levels of the relevant objectives. The basic procedure is to distribute each performance pdf into three bins. The first bin spans the performance range below PMK-R. The second bin spans the performance range between PMK-R and PMK-G. The third bin spans the performance range exceeding PMK-G. This approach focuses the analysis specifically on what is needed to classify the risk as either Red / "Unacceptable," Yellow / "Marginal," or Green / "Acceptable."

Figure 4-14 illustrates the approach. The left-hand side of the figure shows a performance pdf binned according to how much probability is in the region below PMK-R, between PMK-R and PMK-G, and above PMK-G. The right-hand side of the figure shows the CDF associated with the pdf and how it compares to the risk tolerance levels for PMK-R and PMK-G. Based on this information it is possible to classify the risk according to Table 3-II in Part 1 of this handbook, which is reproduced for convenience as Table 4-XII below. The risk to the objective associated with performance measure *X* in Figure 4-14 is classified Yellow / "Marginal" because the CDF falls below IRTL-R in the region below PMK-R but above IRTL-G in the region between PMK-R and PMK-G.

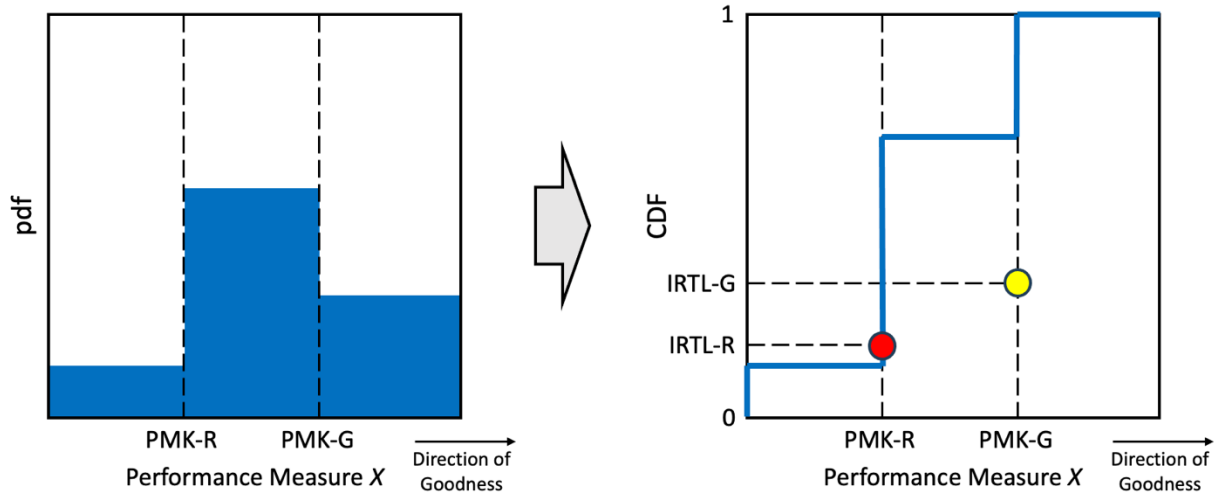


Figure 4-14. Heuristic Approach to Risk Response Analysis of Alternatives

Table 4-XII. Classification of Individual Risks Based on Satisfaction of Individual Risk Tolerance Levels

IRTL-R	IRTL-G	Individual Risk Scenario "Acceptability" Classification
Satisfied	Satisfied	Green / "Acceptable"
Satisfied	Not Satisfied	Yellow / "Marginal"
Not Satisfied	n/a	Red / "Unacceptable"

There is no single method for developing the technical basis for binning the performance pdf into the three bins. At one extreme, there might be statistically robust evidence or thoroughly validated analysis that can be used as a rigorous basis for the binning. At the other extreme, the binning might rely on the qualitative judgement of the analysts and SMEs. Correspondingly, analytical frameworks such as that of Figure 4-13 can be used to produce a network of linked quantitative analytical models, perhaps running within a Monte Carlo shell to propagate the uncertainty in the performance parameters into the performance measure estimates, or they can be used simply to focus thinking on areas of relevance to the subjective assessment of the pdf.

For quantitatively defined IRTLs, comparison of a performance CDF to the relevant IRTL values is straightforward. However, comparison of a performance CDF to qualitative IRTLs such as "Moderate," "Low," or "Very Low" entail a subjective assessment of what counts as "Moderate," "Low," or "Very Low." Ideally, the Acquirer and Provider have a mutual understanding about what the terms mean. Otherwise, it may be prudent for the Provider to confer with the Acquirer to make sure that the Acquirer's risk tolerance levels are understood and that the risk is classified in accordance with Acquirer expectations. In any case, the technical basis for the pdf binning should be documented, defensible, and preserved within the activity's document management system. Where judgement is required, a measure of conservatism should be applied.

Figure 4-15 illustrates the risk acceptability classification process for the *Refurbish* risk response alternative. It shows that the *Refurbish* alternative is affordable and will result in satisfactory though not superior test facility availability for Project "X" and other near-term testing needs. However, the *Refurbish* alternative does little to address Center "Y"'s long-term testing needs or maintain its reputation as a center of testing excellence.

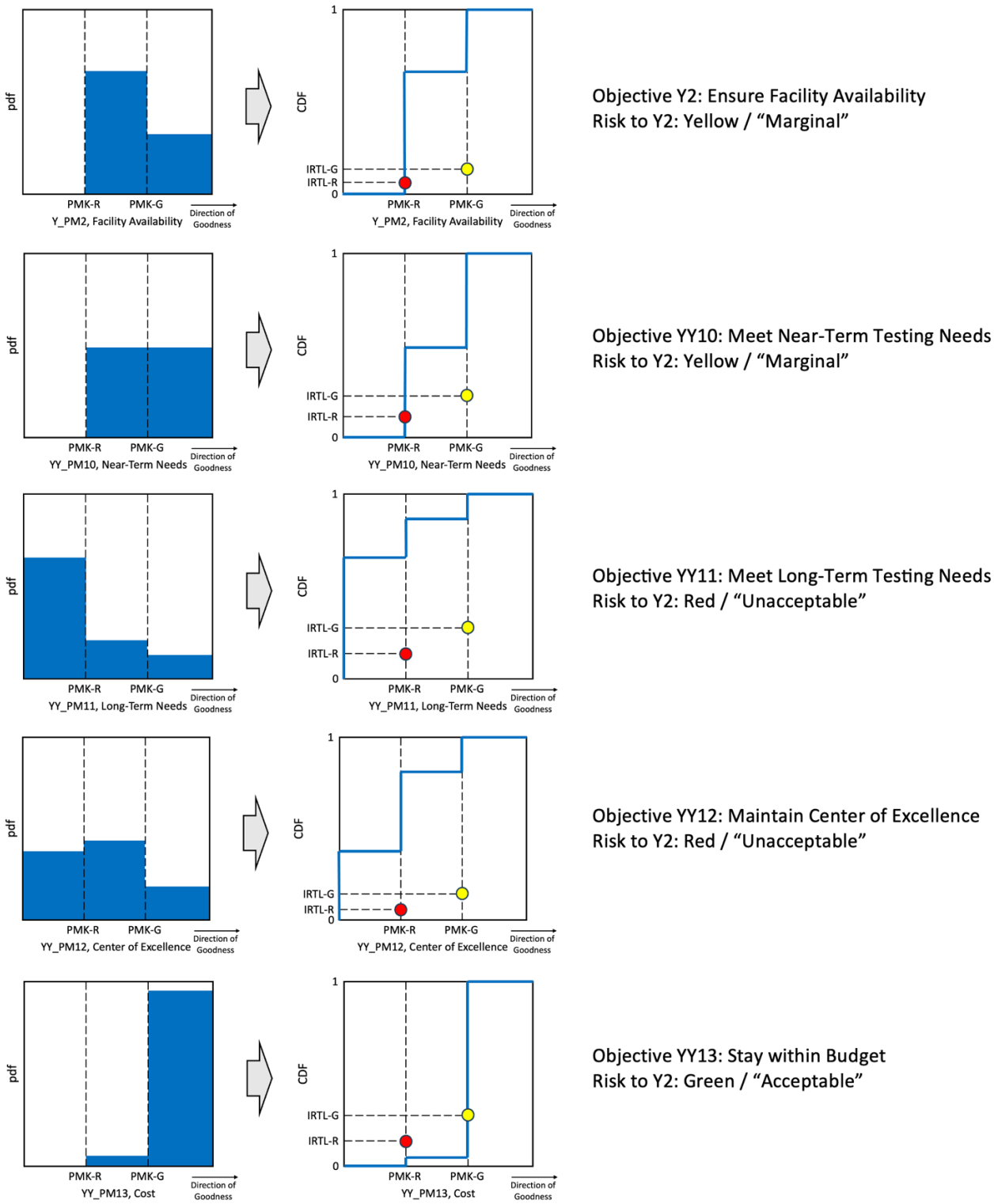


Figure 4-15. Illustrative Risk Acceptability Classifications for the Y_RS2 "Refurbish" Risk Response Alternative

4.5.2.4 Selection of a Risk Response to Risk Y_RS2, Increasing unavailability of Center "Y" test facility due to facility aging

Figure 4-16 presents a spider chart comparing the three risk response alternatives to individual risk scenario Y_RS2 (along with the *No Action* alternative). The chart shows the resulting risks to each of the five affected objectives. Some noteworthy observations that can be quickly made from Figure 4-16 are:

- Although individual risk scenario Y_RS2 was initially identified as a risk to the availability of the Center "Y" test facility to Project "X," the Activity-Execution RIDM analysis brought additional objectives into the picture as part of a holistic analysis of risk.
- Every alternative other than the *No Action* alternative satisfactorily addresses the testing facility availability risks to Project "X" and other users, at least in the short term, although the *Refurbish* alternative falls short of fully addressing the risk to the achievement of the goal availability.
- The *Replace* alternative will reduce the short-term availability risk more than the *Refurbish* alternative will, but at the expense of unacceptable cost risk. Moreover, the *Replace* alternative does not address the risks to the long-term objectives of the facility.
- The *Modernize* alternative effectively addresses the test facility's short-term, long-term, and reputational risks, but at the expense of unacceptable cost risk.

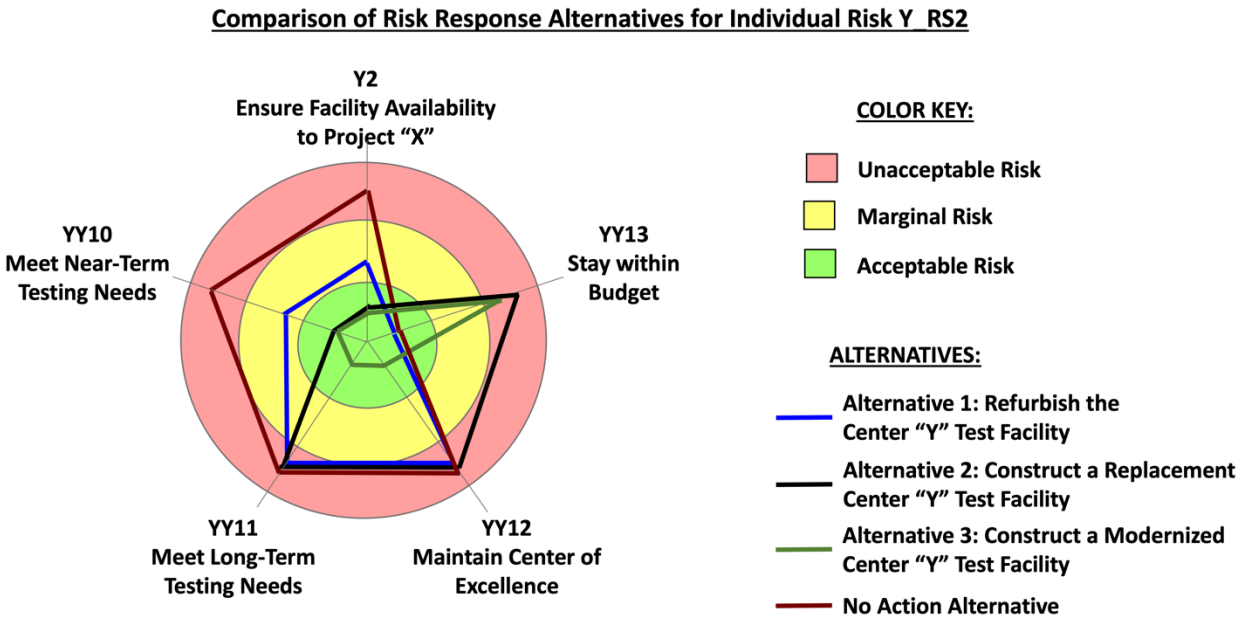


Figure 4-16. Comparison of Risk Response Alternatives for Individual Risk Y_RS2

In this example, two strategies for managing risk Y_RS2 seem reasonable. The first strategy is to focus narrowly on short-term risk by implementing the *Refurbish* alternative, which would also require the spawning of a separate individual risk (or two) to address the unacceptable risks to objectives YY11 and YY12 that would remain even after refurbishment. The other strategy is to

elevate the risk management decision to the level of the Acquirer, who might have the ability to provide the funding needed to implement the *Modernize* alternative without exposing Center "Y" to unacceptable cost risk. This strategy would, for all intents and purposes, transform Y_RS2's Activity-Execution RIDM process into an Activity-Rebaselining RIDM process, as illustrated in Figure 2-9 of Part 1 of this handbook, since at the very least it would entail revision of the performance markers for objective YY13.

There is little reason to consider the *Replace* alternative, since from a risk acceptability perspective the *Modernize* alternative is superior, or at least comparable, for each objective. Similarly, there is little reason to *Accept* the risk, since the *Refurbish* alternative is superior or comparable for each objective.

4.6 References for Chapter 4

1. August 2021 OSMA Risk Management Quarterly Reporting Cycle Executive Overview.
2. NASA Procedural Requirements, NPR 8000.4C, Agency Risk Management Procedural Requirements. April 2022.
3. NASA Special Publication, NASA/SP-2011-3421 Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Second Edition. December 2011.
4. NASA Policy Directive, NPD 1001.0D, 2022 NASA Strategic Plan. March 2022.
5. NASA Cost Estimating Handbook, Version 4.0. February 2015.