How can you support RIDM/CRM/RM through the use of PRA

Supply Chain Conference 2011
Panel Session – NASA's Approach to Integrated Risk Management

Tony DiVenti
Reliability and Risk Analysis Branch – Code 322
Anthony.J.DiVenti@nasa.gov
(301) 286-6507

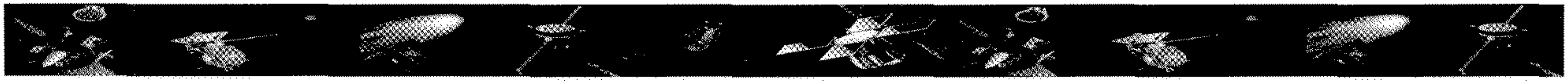
October 19, 2011

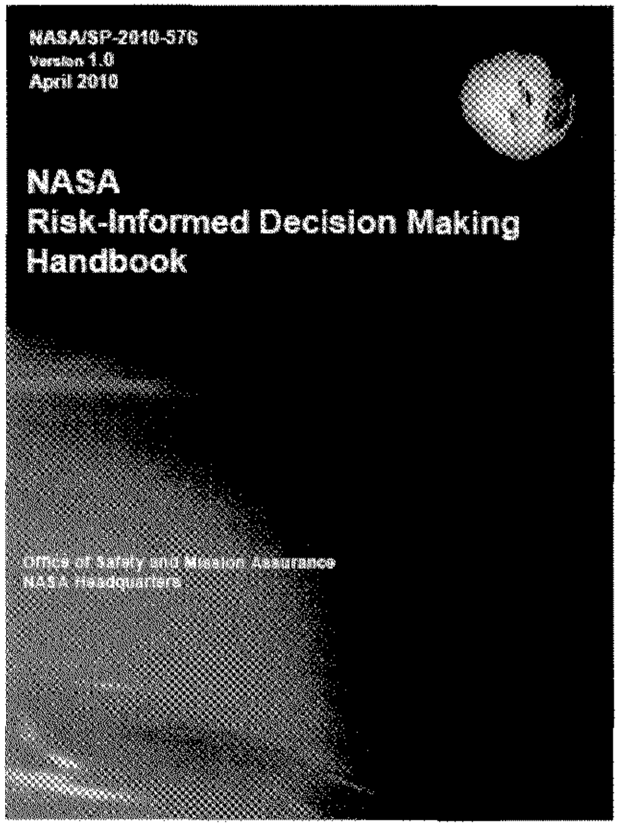
Greenbelt, MD - GSFC

Agenda

- Risk Management (RM) Recap
  - What is Continuous Risk Management (CRM)
  - What is Risk Informed Decision Making (RIDM)
  - What is Risk Management (RM)
- What does PRA mean in the context of RIDM
- NASA's newest PRA requirements
- How does GSFC~~'s~~ flow down PRA requirements
  - Two Approaches
    - In-House PRA Development
    - Out-of-House PRA Development
  - GSFC's Standard Mission Assurance Requirements (MAR) Document
- Discussion

What is RIDM?

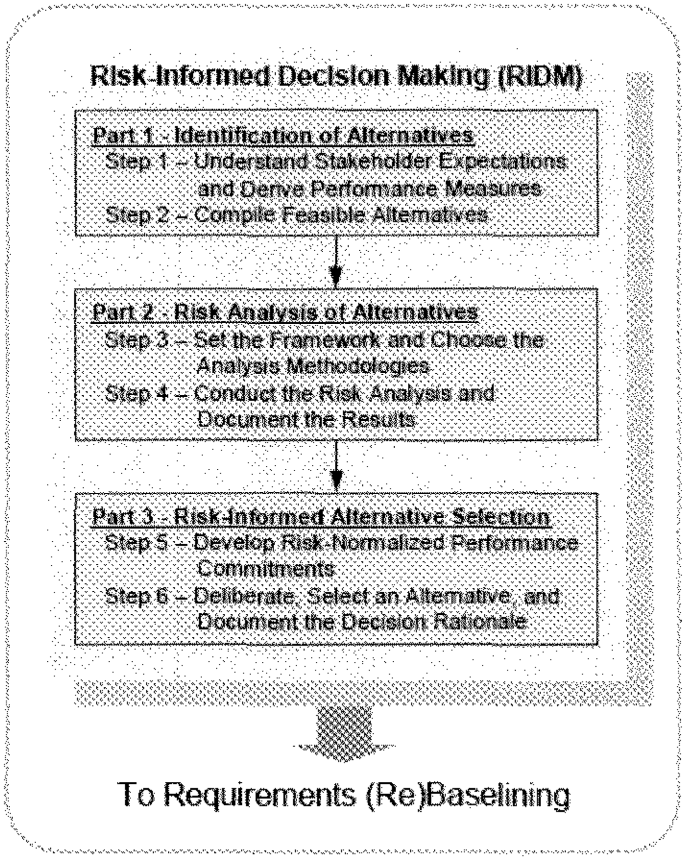




NASA/SP-2010-576
Version 1.0
April 2010

NASA
Risk-Informed Decision Making
Handbook

Office of Safety and Mission Assurance
NASA Headquarters



Risk-Informed Decision Making (RIDM)

Part 1 - Identification of Alternatives
Step 1 – Understand Stakeholder Expectations and Derive Performance Measures
Step 2 – Compile Feasible Alternatives

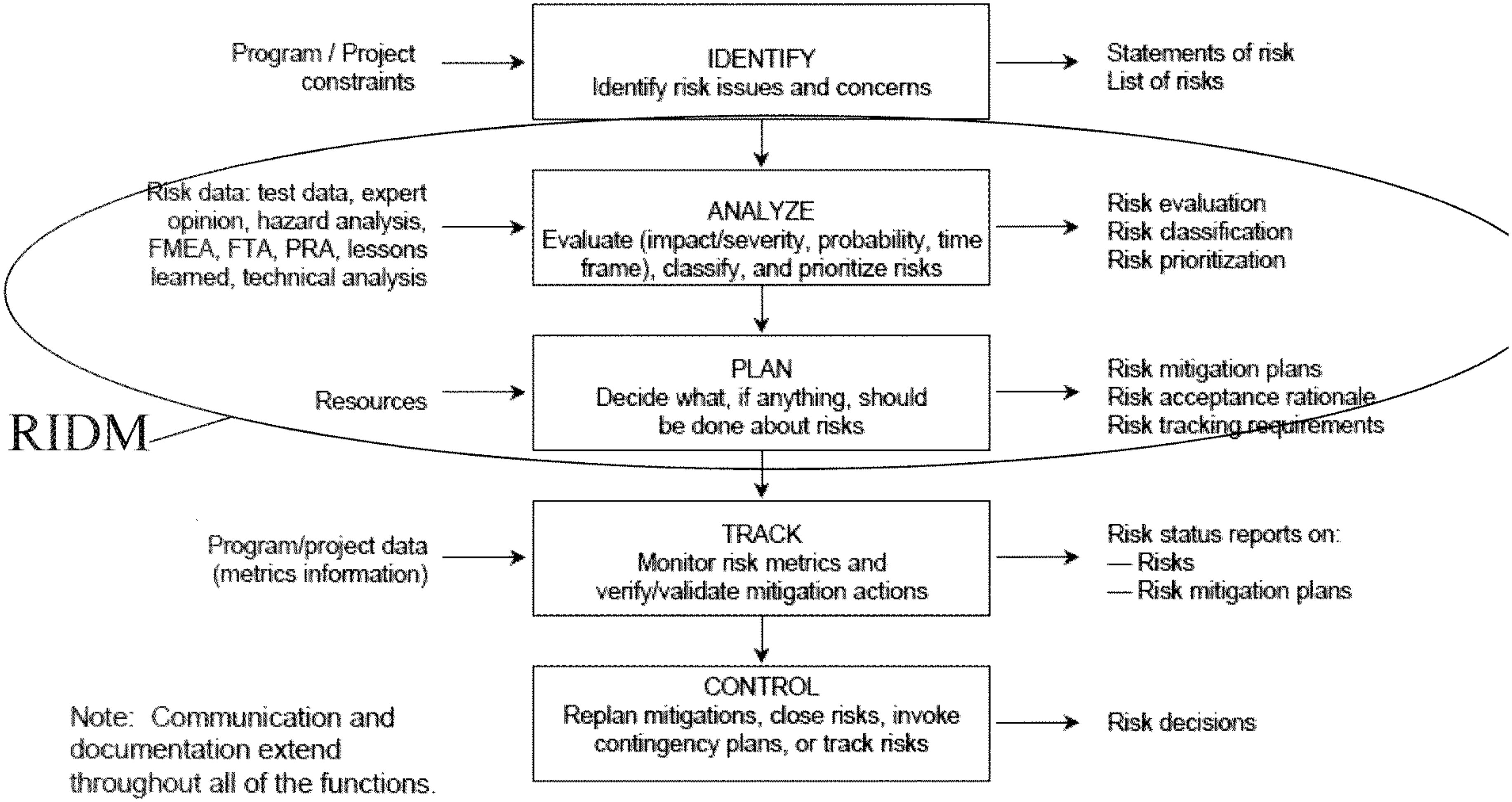
Part 2 - Risk Analysis of Alternatives
Step 3 – Set the Framework and Choose the Analysis Methodologies
Step 4 – Conduct the Risk Analysis and Document the Results

Part 3 - Risk-Informed Alternative Selection
Step 5 – Develop Risk-Normalized Performance Commitments
Step 6 – Deliberate, Select an Alternative, and Document the Decision Rationale

To Requirements (Re)Baselining

http://www.hq.nasa.gov/office/codeq/doctree/SP2010576.htm

Continuous Risk Management (CRM)



Program / Project constraints → IDENTIFY
Identify risk issues and concerns → Statements of risk
List of risks

Risk data: test data, expert opinion, hazard analysis, FMEA, FTA, PRA, lessons learned, technical analysis → ANALYZE
Evaluate (impact/severity, probability, time frame), classify, and prioritize risks → Risk evaluation
Risk classification
Risk prioritization

Resources → PLAN
Decide what, if anything, should be done about risks → Risk mitigation plans
Risk acceptance rationale
Risk tracking requirements

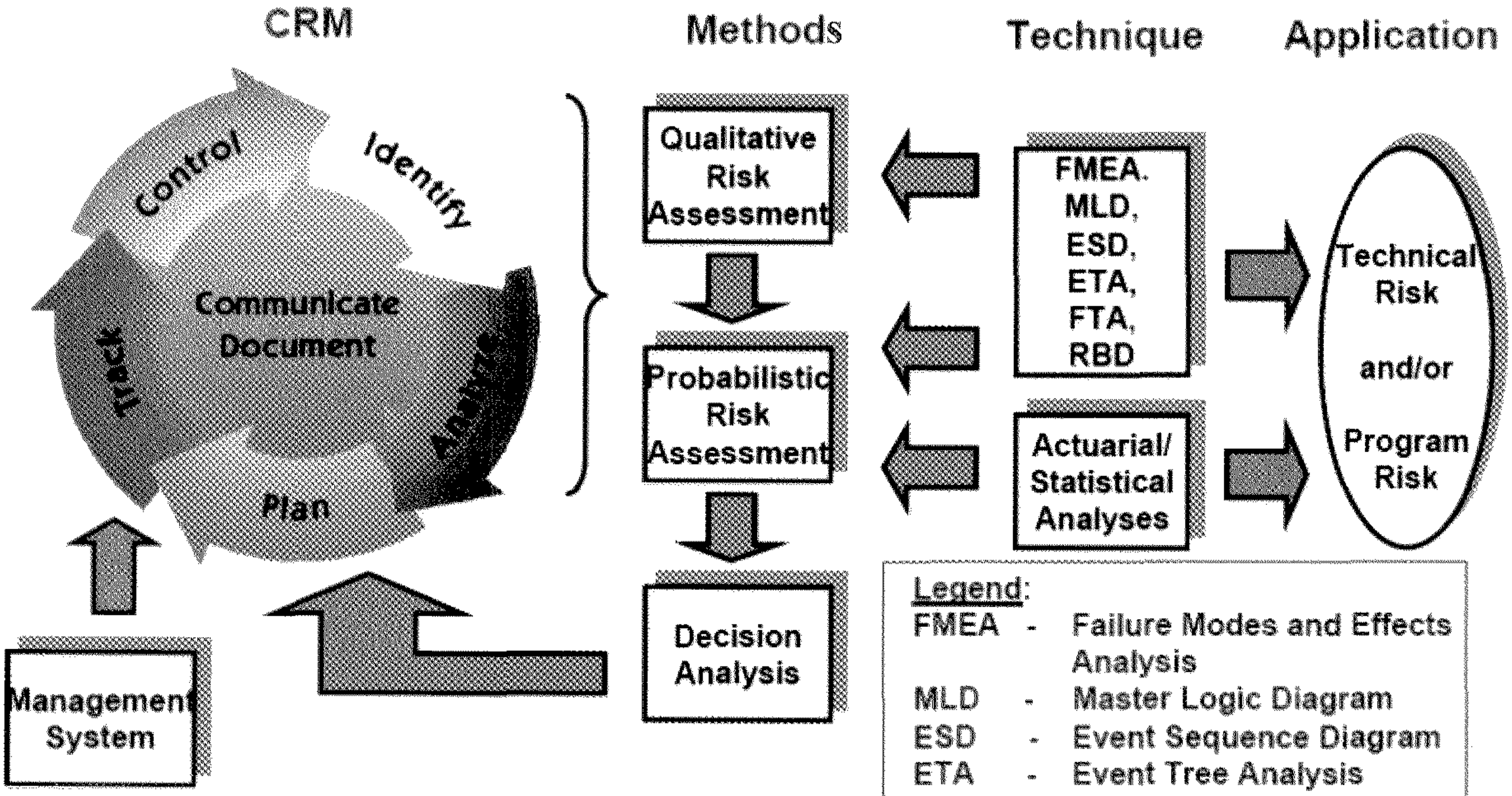
RIDM

Program/project data (metrics information) → TRACK
Monitor risk metrics and verify/validate mitigation actions → Risk status reports on:
— Risks
— Risk mitigation plans

CONTROL
Replan mitigations, close risks, invoke contingency plans, or track risks → Risk decisions

Note: Communication and documentation extend throughout all of the functions.

What is Risk Management?



CRM

Control

Identify

Communicate
Document

Track

Analyze

Plan

Management System

Methods

Qualitative Risk Assessment

Probabilistic Risk Assessment

Decision Analysis

Technique

FMEA, MLD, ESD, ETA, FTA, RBD

Actuarial/ Statistical Analyses

Application

Technical Risk

and/or

Program Risk

Legend:

FMEA	-	Failure Modes and Effects Analysis
MLD	-	Master Logic Diagram
ESD	-	Event Sequence Diagram
ETA	-	Event Tree Analysis
FTA	-	Fault Tree Analysis
RBD	-	Reliability Block Diagram

Diagram taken from Source 7

What is PRA?

Definition:

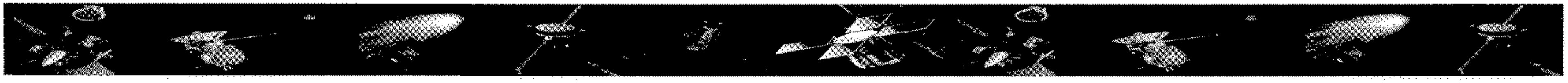
Probabilistic Risk Assessment (PRA) is one of the key RIDM tools. It is a scenario-based methodology aimed at identifying and assessing Safety and Technical Performance risks in complex technological systems.

PRA characterizes:

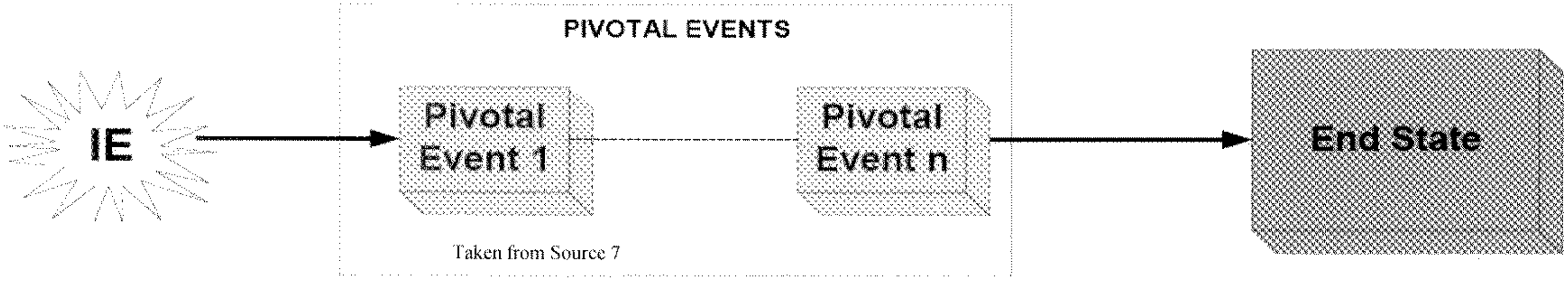
1) What can go wrong?
2) How likely is it?
3) What are the consequences

Triplet Concept: Scenario, Likelihood, Impact

What is PRA?



PRA Scenario Concept:



PIVOTAL EVENTS

IE

Pivotal Event 1

Pivotal Event n

End State

Taken from Source 7

Source of Initiating Event:

- FMEAs
- HazReps
- Failure History
- Master Logic Diagram

Source of Pivotal Events:

Same as IEs, plus

- Ground Procedures
- Crew Procedures
- Automatic emergency systems, etc.

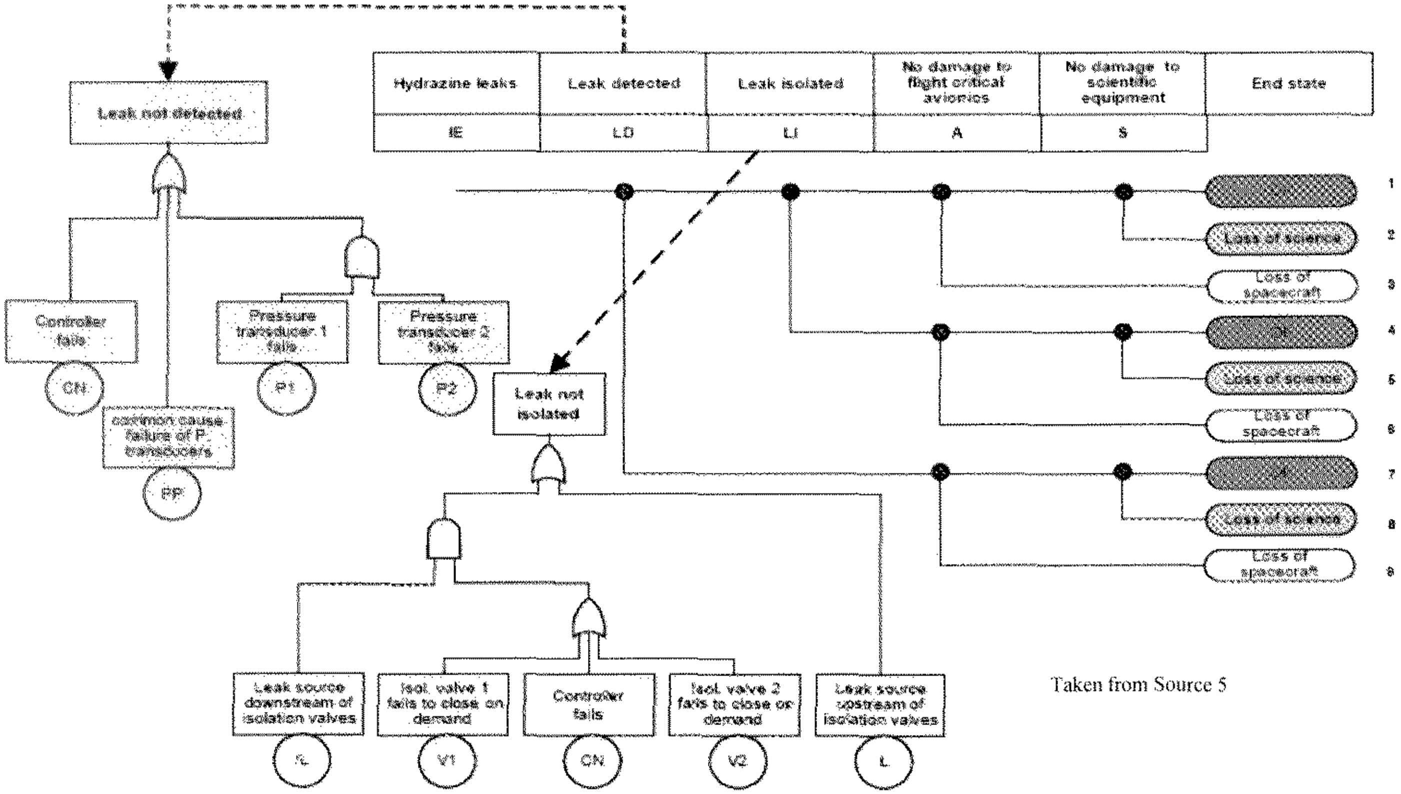
End State:

Detrimental consequence of interest

Accident Scenario is a string of events that, if it occurs, will lead to an undesired end state.

What is PRA?

What makes PRA appealing is its ability to integrate several sources of information together that may contribute to Risk.

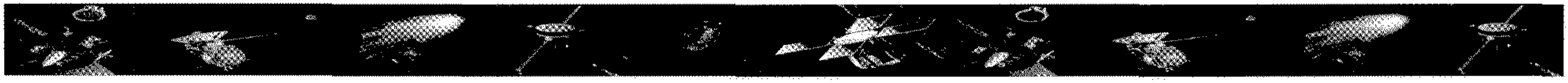


Hydrazine leaks	Leak detected	Leak isolated	No damage to flight critical avionics	No damage to scientific equipment	End state
IE	LD	LI	A	S	

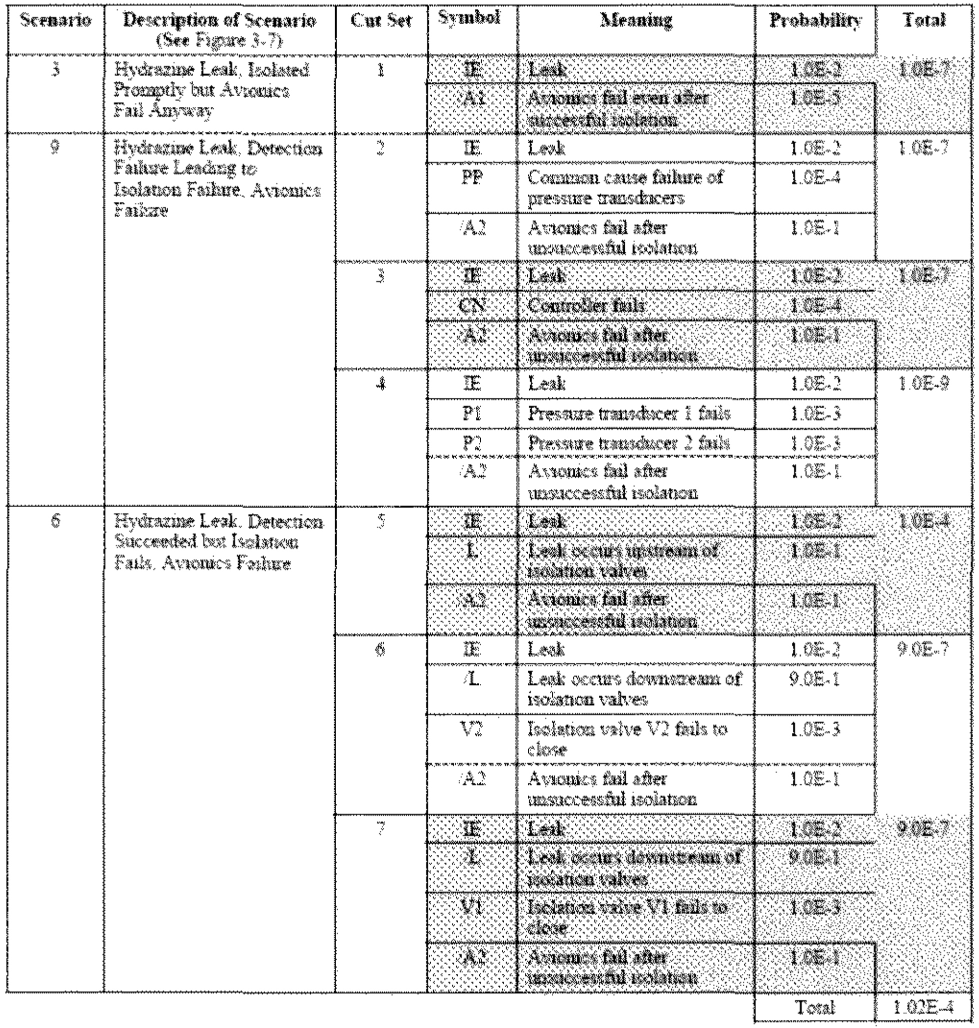
Leak not detected
Controller fails
CN
common cause failure of P. transducers
PP
Pressure transducer 1 fails
P1
Pressure transducer 2 fails
P2
Leak not isolated
Leak source downstream of isolation valves
/L
Isol. valve 1 fails to close on demand
V1
Controller fails
CN
Isol. valve 2 fails to close on demand
V2
Leak source upstream of isolation valves
L
1
Loss of science
2
Loss of spacecraft
3
4
Loss of science
5
Loss of spacecraft
6
7
Loss of science
8
Loss of spacecraft
9

Taken from Source 5

What is PRA?



The integrated risk scenario model allows for a robust and ordered ranking of the risk contributors that may lead to the undesired states of interest



Scenario	Description of Scenario (See Figure 3-7)	Cut Set	Symbol	Meaning	Probability	Total
3	Hydrazine Leak, Isolated Promptly but Avionics Fail Anyway	1	IE	Leak	1.0E-2	1.0E-7
			/A1	Avionics fail even after successful isolation	1.0E-5	
9	Hydrazine Leak, Detection Failure Leading to Isolation Failure, Avionics Failure	2	IE	Leak	1.0E-2	1.0E-7
			PP	Common cause failure of pressure transducers	1.0E-4	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		3	IE	Leak	1.0E-2	1.0E-7
			CN	Controller fails	1.0E-4	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		4	IE	Leak	1.0E-2	1.0E-9
			P1	Pressure transducer 1 fails	1.0E-3	
			P2	Pressure transducer 2 fails	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
6	Hydrazine Leak, Detection Succeeded but Isolation Fails, Avionics Failure	5	IE	Leak	1.0E-2	1.0E-4
			L	Leak occurs upstream of isolation valves	1.0E-1	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		6	IE	Leak	1.0E-2	9.0E-7
			/L	Leak occurs downstream of isolation valves	9.0E-1	
			V2	Isolation valve V2 fails to close	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
		7	IE	Leak	1.0E-2	9.0E-7
			/L	Leak occurs downstream of isolation valves	9.0E-1	
			V1	Isolation valve V1 fails to close	1.0E-3	
			/A2	Avionics fail after unsuccessful isolation	1.0E-1	
					Total	1.02E-4

Taken from Source 5

Two-Sets of Requirements governing PRA activity at GSFC

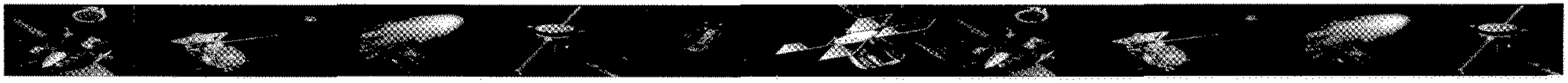
Applicable requirements pulled from:

- NPR 8705.5A PRA Procedures for NASA Programs and Projects (2010)
- NPR 8715.3C NASA General Safety Program Requirements (2012)

Some of the Significant Changes to NPR 8705.5 made in conjunction with RIDM

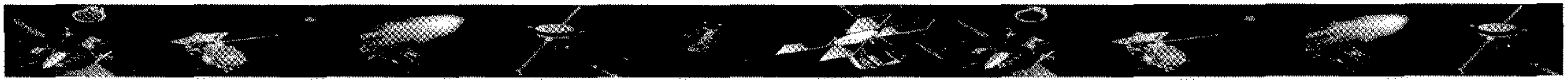
- Removed language addressing Full, Simplified, and Limited Scope PRA.
- Greater emphasis on PRA Planning/PRA Plan Documentation
  - Formal PRA Plan shall be developed by PRA Lead and approved by Program/Project Manager to:
    - Identify specific end-states (undesirable consequences, performance measures, figures of merit) of interest consistent with PRA objectives
    - Define quantitative performance measures and numerical criteria that are to be evaluated by the PRA consistent with objectives
    - Develop a PRA schedule compatible with objectives, applications, and life cycle phases approved by the Program/Project manager
- Greater tie-in with Program/Project characterization of NPR 7120.5 NASA Space Flight Program and Project Management Requirements
  - Use of Category 1 (i.e., LCC greater than 1 Billion dollars, Nuclear Payloads, Human Spaceflight)

New NPR 8705.5 Requirements for GSFC



- Formal submittal of PRA Decisions – Cat I and Cat II, Class A or Class B.
- Formal submittal of PRA plans, including scope and rationale
- Requires Program Manager approval (note: PRA decision/scope determination is the primary responsibility of the Project subject to OSMA/Center SMA Concurrence)
- Formal coordination of Independent PRA Review with OSMA.

How is GSFC Flowing Down PRA Requirements to Developers/Suppliers



- GSFC’s Mission Assurance Requirements (MAR)

PROBABILISTIC RISK ANALYSIS (PRA) AND RELIABILITY

Tailoring note: The PRA and reliability engineering section requires tailoring per the classification requirements of NPR 8705.4, NPR 8705.5, and project-specific requirements.

RELIABILITY PROGRAM PLAN

Tailoring note: If PRA is being invoked in section 4.2, change section 4.1to read from “...implement a Reliability Program Plan (RPP)” to “...”implement a Reliability Program Plan, including the developer’s approach to PRA requirements in section 4.2, ..”

The developer shall document and implement a Reliability Program Plan (RPP) using both qualitative and quantitative techniques to support decisions regarding mission success and safety throughout system development. The RPP shall include a detailed approach to the analysis of hardware and software for their contributions to system reliability and mission success. The developer shall present the implementation of these plans and related activities at milestone reviews beginning with the System Requirements Review (DID 4-1).

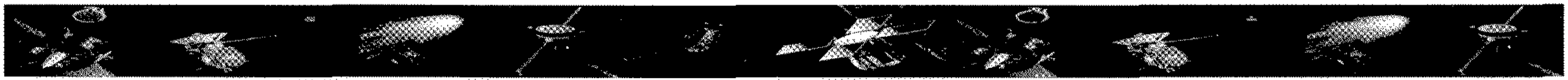
PROBABILISTIC RISK ASSESSMENT

Tailoring notes: See paragraph 2.2.1a of NPR 8705.5 for criteria regarding the requirement to perform a PRA. If a PRA is not required, delete this section and the related DIDs. If a PRA will be performed, delete the non-applicable paragraph and related DID.

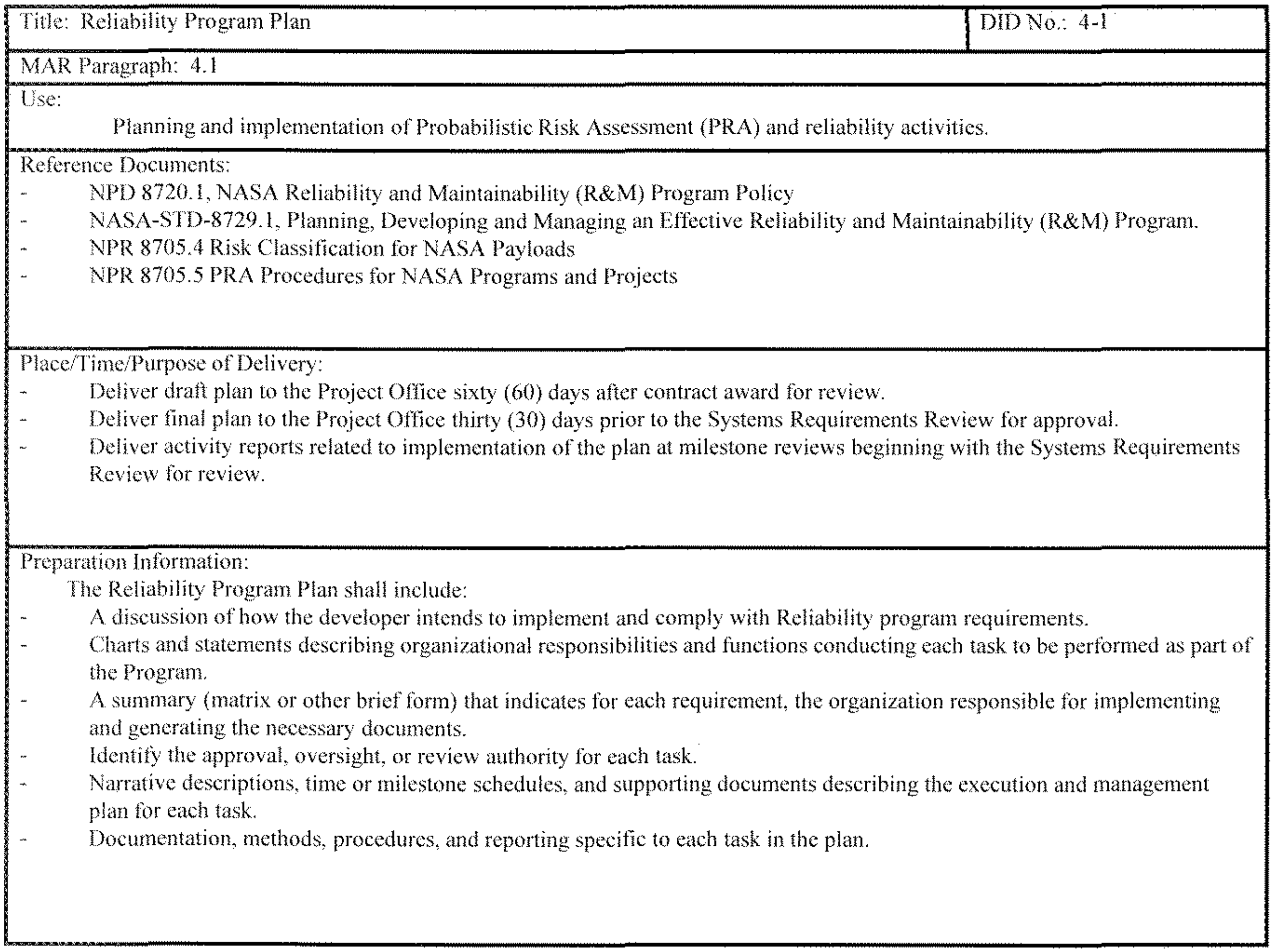
The developer shall perform a Probabilistic Risk Assessment in accordance with NPR 8705.5, Probabilistic Risk Assessment (PRA) Technical Procedures for Safety and Mission Success for NASA Programs and Projects (DID 4-2).

The developer shall provide the information for a Probabilistic Risk Assessment per NPR 8705.5, Probabilistic Risk Assessment (PRA) Technical Procedures for Safety and Mission Success for NASA Programs and Projects (DID 4-2).

How is GSFC Flowing Down PRA Requirements to Developers/Suppliers



- MAR Data Items Description (DID 4-1)



Title: Reliability Program Plan	DID No.: 4-1

MAR Paragraph: 4.1

Use:

Planning and implementation of Probabilistic Risk Assessment (PRA) and reliability activities.

Reference Documents:

- NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy
- NASA-STD-8729.1, Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program.
- NPR 8705.4 Risk Classification for NASA Payloads
- NPR 8705.5 PRA Procedures for NASA Programs and Projects

Place/Time/Purpose of Delivery:

- Deliver draft plan to the Project Office sixty (60) days after contract award for review.
- Deliver final plan to the Project Office thirty (30) days prior to the Systems Requirements Review for approval.
- Deliver activity reports related to implementation of the plan at milestone reviews beginning with the Systems Requirements Review for review.

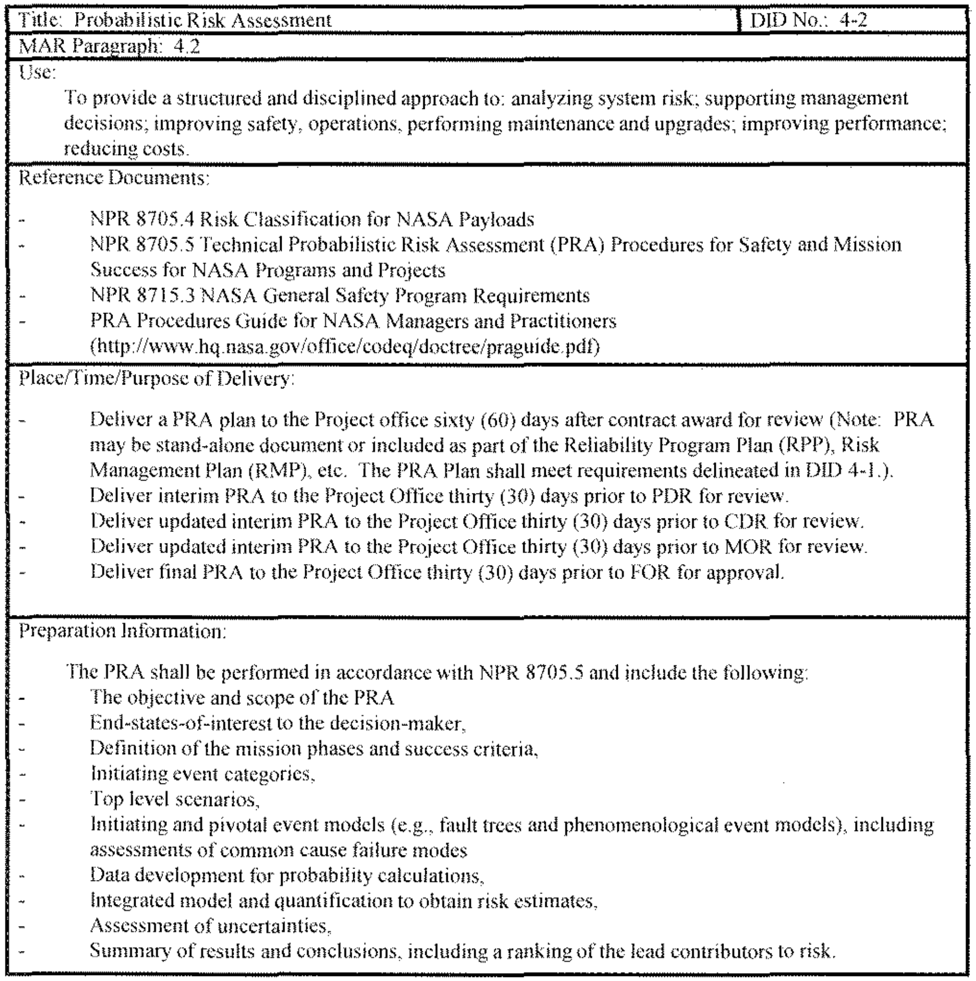
Preparation Information:

The Reliability Program Plan shall include:

- A discussion of how the developer intends to implement and comply with Reliability program requirements.
- Charts and statements describing organizational responsibilities and functions conducting each task to be performed as part of the Program.
- A summary (matrix or other brief form) that indicates for each requirement, the organization responsible for implementing and generating the necessary documents.
- Identify the approval, oversight, or review authority for each task.
- Narrative descriptions, time or milestone schedules, and supporting documents describing the execution and management plan for each task.
- Documentation, methods, procedures, and reporting specific to each task in the plan.

How is GSFC Flowing Down PRA Requirements to Developers/Suppliers

MAR DID 4-1 – ***use this DID if the developer is performing the PRA***



Title: Probabilistic Risk Assessment	DID No.: 4-2

MAR Paragraph: 4.2

Use:

To provide a structured and disciplined approach to: analyzing system risk; supporting management decisions; improving safety, operations, performing maintenance and upgrades; improving performance; reducing costs.

Reference Documents:

- NPR 8705.4 Risk Classification for NASA Payloads
- NPR 8705.5 Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects
- NPR 8715.3 NASA General Safety Program Requirements
- PRA Procedures Guide for NASA Managers and Practitioners (http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf)

Place/Time/Purpose of Delivery:

- Deliver a PRA plan to the Project office sixty (60) days after contract award for review (Note: PRA may be stand-alone document or included as part of the Reliability Program Plan (RPP), Risk Management Plan (RMP), etc. The PRA Plan shall meet requirements delineated in DID 4-1.).
- Deliver interim PRA to the Project Office thirty (30) days prior to PDR for review.
- Deliver updated interim PRA to the Project Office thirty (30) days prior to CDR for review.
- Deliver updated interim PRA to the Project Office thirty (30) days prior to MOR for review.
- Deliver final PRA to the Project Office thirty (30) days prior to FOR for approval.

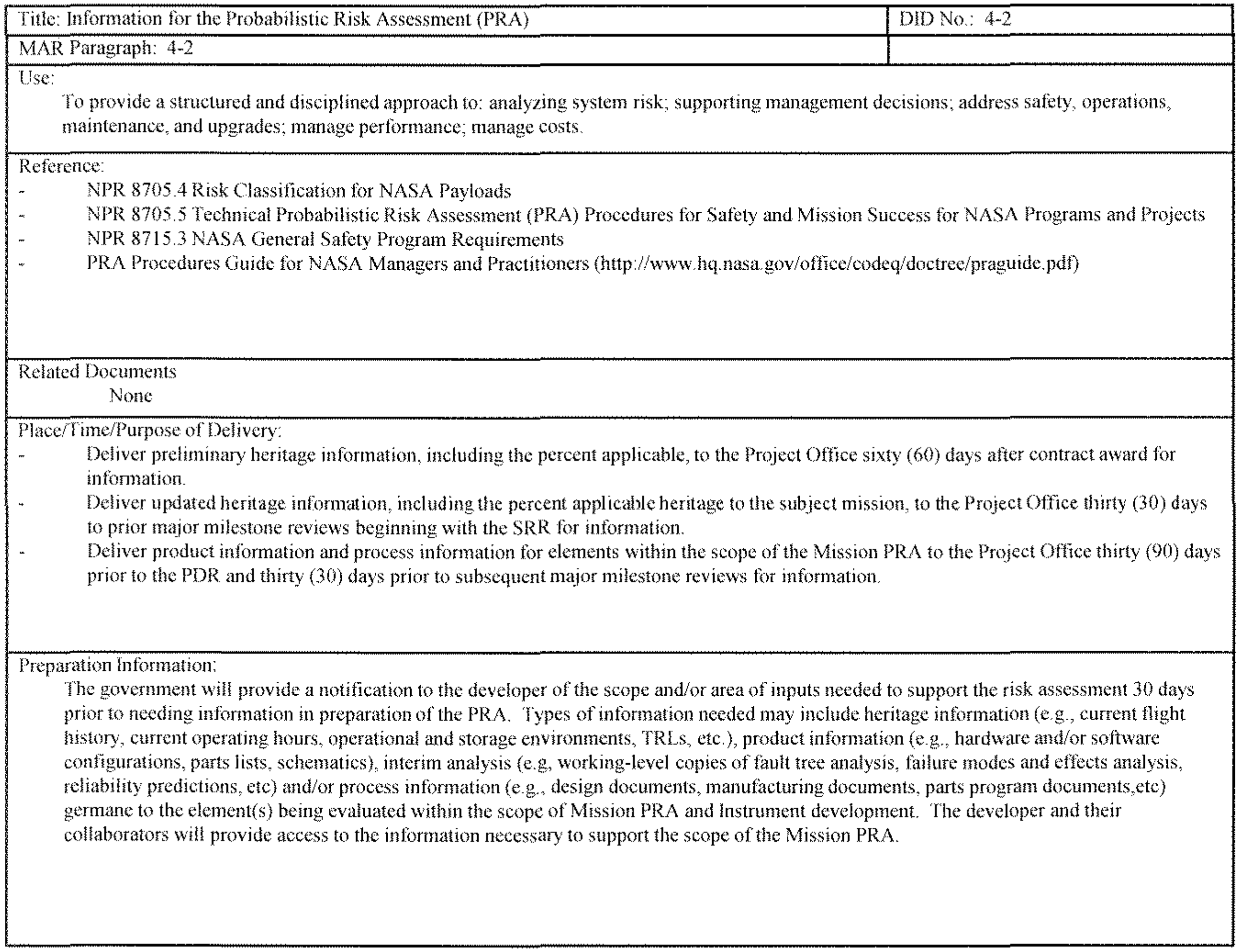
Preparation Information:

The PRA shall be performed in accordance with NPR 8705.5 and include the following:

- The objective and scope of the PRA
- End-states-of-interest to the decision-maker,
- Definition of the mission phases and success criteria,
- Initiating event categories,
- Top level scenarios,
- Initiating and pivotal event models (e.g., fault trees and phenomenological event models), including assessments of common cause failure modes
- Data development for probability calculations,
- Integrated model and quantification to obtain risk estimates,
- Assessment of uncertainties,
- Summary of results and conclusions, including a ranking of the lead contributors to risk.

How is GSFC Flowing Down PRA Requirements to Developers/Suppliers

MAR DID 4-2 – *use this DID if the GSFC is performing the PRA*

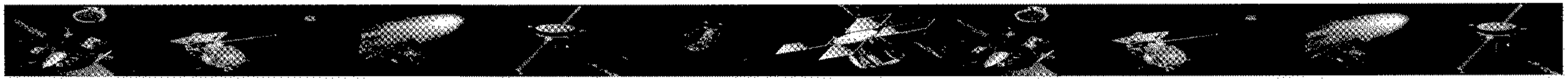


Title: Information for the Probabilistic Risk Assessment (PRA)	DID No.: 4-2
MAR Paragraph: 4-2	
Use: To provide a structured and disciplined approach to: analyzing system risk; supporting management decisions; address safety, operations, maintenance, and upgrades; manage performance; manage costs.	
Reference: - NPR 8705.4 Risk Classification for NASA Payloads - NPR 8705.5 Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects - NPR 8715.3 NASA General Safety Program Requirements - PRA Procedures Guide for NASA Managers and Practitioners (http://www.hq.nasa.gov/office/codeq/doctree/praguide.pdf)	
Related Documents None	
Place/Time/Purpose of Delivery: - Deliver preliminary heritage information, including the percent applicable, to the Project Office sixty (60) days after contract award for information. - Deliver updated heritage information, including the percent applicable heritage to the subject mission, to the Project Office thirty (30) days to prior major milestone reviews beginning with the SRR for information. - Deliver product information and process information for elements within the scope of the Mission PRA to the Project Office thirty (90) days prior to the PDR and thirty (30) days prior to subsequent major milestone reviews for information.	
Preparation Information: The government will provide a notification to the developer of the scope and/or area of inputs needed to support the risk assessment 30 days prior to needing information in preparation of the PRA. Types of information needed may include heritage information (e.g., current flight history, current operating hours, operational and storage environments, TRLs, etc.), product information (e.g., hardware and/or software configurations, parts lists, schematics), interim analysis (e.g, working-level copies of fault tree analysis, failure modes and effects analysis, reliability predictions, etc) and/or process information (e.g., design documents, manufacturing documents, parts program documents,etc) germane to the element(s) being evaluated within the scope of Mission PRA and Instrument development. The developer and their collaborators will provide access to the information necessary to support the scope of the Mission PRA.	

Lessons Learned

- It is important that a clear scope, set of objectives, and milestones be established upfront with the project team to help ensure that needed questions will be answered in a timely manner.
- PRA and other models rely heavily on the degree and fidelity to which they match what will happen in reality. Such modeling requires close coordination with the design team, and a sound system understanding from the modeler.
- Need to establish a framework for developing basic event likelihood distributions upfront.
- Need to clearly communicate results

Discussion



- Comments
- Questions