



Goddard Procedures and Guidelines

DIRECTIVE NO. GPG 7120.4
EFFECTIVE DATE: December 7, 2001
EXPIRATION DATE: December 7, 2006

APPROVED BY Signature: Original signed by
NAME: A. V. Diaz
TITLE: Director

Responsible Office: Code 300/Office of System Safety and Mission Assurance, Systems Management Office

Title: Risk Management

PREFACE

P.1 PURPOSE

Risk management is an organized, systematic decision-making process that efficiently identifies, analyzes, plans (for the handling of risks), tracks, controls, communicates, and documents risks to increase the likelihood of achieving program/project goals. This GPG provides procedures and guidelines for applying risk management to GSFC projects as required by NPG 7120.5, "Program and Project Management Processes and Requirements."

P.2 APPLICABILITY

This risk management procedure shall be applied to all space flight systems (e.g., projects) for which GSFC is responsible. This procedure shall also be applied to deliverable instruments, spacecraft and other GSFC products designated by the GSFC Center Director. This procedure applies to project formulation and implementation subprocesses, including mission operations.

The formal risk management requirements defined in this GPG do not apply to sounding rockets, balloons, and aircraft or their associated instruments/payloads. Small Shuttle Payloads (e.g., Hitchhiker, Space Experiment Module, and Get-Away-Specials) are also excluded. However, product managers for these types of missions shall define and implement an effective risk management process commensurate with the level of risk associated with their specific missions.

P.3 AUTHORITY

NPD 7120.4, Program/Project Management

P.4 REFERENCES

- a. NPG 7120.5, Program and Project Management Processes and Requirements
- b. NPG 8715.3, NASA Safety Manual
- c. NASA Federal Acquisition Regulations (FAR) Supplement (NFS) Parts 1807, 1815, 1823, and 1846.
- d. GPG 8700.4, Integrated Independent Reviews.

- e. GPG 1060.2 - Management Review And Reporting for Programs and Projects.
- f. Risk Management training, tools, techniques, and case studies as applied to NASA projects, available at <http://smo.gsfc.nasa.gov/>

P.5 CANCELLATION

None

P.6 SAFETY

None

P.7 TRAINING

Project teams shall be trained in Continuous Risk Management as defined in paragraph 2.4.

P.8 RECORDS

None

P.9 METRICS

None

P.10 DEFINITIONS

- a. Risk - Risk is the combination of the probability that a project will experience an undesired event (e.g., safety mishap, environmental exposure, failure to achieve mission success criteria, cost overrun, schedule slippage, etc.) and the consequences, impact, or severity of the undesired event, were it to occur.
- b. Acceptable Risk – Acceptable risk is the risk that is understood and agreed to by the program/project, Governing Program Management Council (GPMP), Enterprise and other customer(s) sufficient to achieve the defined success criteria within the approved level of resources.
- c. Primary Risk – A Primary Risk is a risk that is assessed as both a high probability and high impact/severity.
- d. Risk Management - Risk Management is a process wherein the project manager leads the project team in identifying, analyzing, planning, tracking, controlling, and communicating the risks and the actions to handle them. Effective communication must occur within the team and with management and customers. Risk management is driven by established success criteria. As depicted in Figure 1, risk management is a continuous, iterative process to manage risk in order to achieve safety and mission

success. Continuous Risk Management (CRM) is an essential element and an integral part of NASA project management and system engineering.

- e. Risk List – The Risk List is the listing of all identified risks in priority order from highest to lowest risk, together with the information that is needed to manage each risk and document its evolution over the course of the project.
- f. Risk-Based Acquisition Management – Risk Based Acquisition Management (RBAM) is a management initiative to apply CRM earlier and throughout the acquisition process (i.e., requirements development, acquisition planning, RFP development/solicitation, source selection, and post-award acquisition management).
- g. Failure Modes and Effects Analysis (FMEA) - A Failure Modes and Effects Analysis is a procedure by which each potential failure mode of each element of a system is analyzed to determine the effects of the failure mode on the system and to classify each potential failure mode according to the severity of the effects.

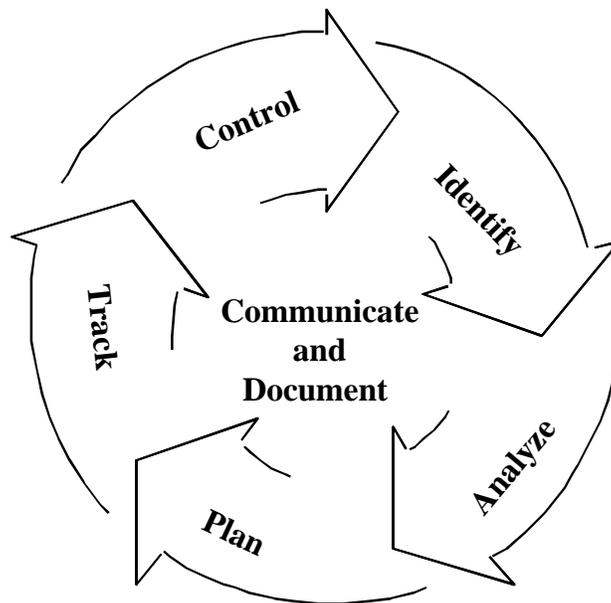


Figure 1. Continuous Risk Management (CRM)

- h. Fault Tree Analysis (FTA) - A Fault Tree Analysis is a qualitative technique to uncover credible ways that a top event (undesired) can occur. The results of the FTA are documented in a fault tree, which is a graphical representation of the combination of faults that will result in the occurrence of undesired top event.
- i. Probabilistic Risk Assessment (PRA) - Probabilistic Risk Assessment is a rigorous technical discipline used in complex technological applications to reveal design, operation and maintenance vulnerabilities, to enhance safety and to reduce costs.

DIRECTIVE NO.	<u>GPG 7120.4</u>
EFFECTIVE DATE:	<u>December 7, 2001</u>
EXPIRATION DATE:	<u>December 7, 2006</u>

PROCEDURES

1. Roles and Responsibilities

1.1 The product manager for the system development activity, typically a Project Formulation Manager, Project Manager or Instrument Manager, shall lead the Continuous Risk Management (CRM) process across the full scope of the product development activity. That leader, hereafter referred to as the Project Manager (PM), is ultimately responsible for identifying, collecting, verifying, and prioritizing risks; making risk mitigation and acceptance decisions; monitoring risk mitigation plans; and reporting the results of CRM to higher level management. The PM defines and documents the project unique aspects of the CRM process and assigns responsibility to team members for CRM implementation. The PM makes the risk tradeoffs across the project team.

1.2 The PM shall assign specific responsibilities for CRM implementation to project team members as the PM judges to be appropriate. Each major element and/or subsystem lead is expected to play a key role in the management of the technical and programmatic risks specific to their area of responsibility and actively participate in system-level risk management activities. The PM may also assign individuals to conduct additional risk management activities that cross multiple areas.

1.3 The implementation of many aspects and activities of CRM, and the orchestration of the various influencing requirements are inherent and inclusive within the systems engineering process. Typically, the Mission Systems Engineer (MSE), or equivalent is tasked by the PM to define and implement a systems engineering approach for the project that integrates the CRM process. This implementation includes the use of risk assessment tools and methodologies to support the qualitative and quantitative assessment of risk inherent within the system. The MSE leads the conduct and integration of technical risk assessments, system analyses and trade studies consistent with the mission success criteria and acceptable risk established for the project. The Systems Safety and Reliability Office (Code 302) provides support to the MSE in the conduct and evaluation of technical risk analyses such as FMEA, FTA, and PRA.

1.4 Similarly, the implementation of many aspects and activities of risk management, and the orchestration of the various influencing requirements, are inherent and inclusive within the safety and mission assurance process. The Systems Assurance Manager (SAM) and Systems Safety Manager assigned to the project management team shall define the safety and mission assurance requirements and manage the related surveillance activities necessary to effectively assess and manage risks.

1.5 The GSFC Program Management Council (PMC) concurs with the mission success criteria and acceptable risk and verifies that resources are adequate as part of the confirmation process. The PMC reviews the residual risks relative to the success criteria and acceptable risk as part of the monthly status and mission readiness review processes. See GPG 1060.2 for further information on these PMC processes.

1.6 The GSFC Systems Management Office (SMO) is responsible to the Center Director for risk management policy, procedures, guidelines and best practices. The SMO shall concur with the project Risk Management Plan. The SMO shall assess CRM planning and implementation as a key objective of the Integrated Independent Reviews (GPG 8700.4) conducted in support of the PMC. The SMO also

DIRECTIVE NO.	<u>GPG 7120.4</u>
EFFECTIVE DATE:	<u>December 7, 2001</u>
EXPIRATION DATE:	<u>December 7, 2006</u>

has the Agency-level responsibility for CRM training and provides risk management consultation to NASA program/project teams.

2. Requirements

2.1 GSFC projects shall implement a systems management approach that formalizes and integrates the CRM process throughout the system life cycle. All elements of the system shall be addressed (e.g., flight, ground and launch vehicle segments, hardware and software, critical ground support equipment). All phases of the life cycle shall be considered (e.g., fabrication, assembly, integration and test, environmental testing, transportation, launch site processing, launch deployment, in-orbit check out, operations decommissioning).

This implementation shall include the use of tools and methodologies to support the qualitative and quantitative assessment of risk inherent in the system design and associated development and operations activities. FMEA's, FTA's and PRA's are conducted as part of the system design, analysis and trade study activities. The results of these risk assessments shall be used to support project management decisions with respect to safety and mission success, and programmatic commitments.

2.2 GSFC projects shall incorporate the requirements of the Risk-Based Acquisition Management (RBAM) initiative as part of the CRM process. The purpose of RBAM is to convey NASA's focus on safety and mission success to NASA contractors.

- a. Acquisition planning shall incorporate input from GSFC personnel responsible for safety and mission assurance, health, environmental protection, information technology, export control, and security.
- b. When technical proposals are required as part of requests for proposals for supplies or services, offerors shall be instructed to identify and discuss risk factors and their approach for managing those risk factors (see NFS 1815.201 and NSF 1815.203-72). Where the solicitation requires submission of a Safety and Health Plan (see NFS 1823.7001(c)), safety and health shall be considered in the evaluation process (also see NFS 1815.305).
- c. Quality assurance surveillance plans are required and prepared with the statement of work for all performance-based contracts and, as necessary, for other contracts. Those plans shall reflect the project-specific surveillance approach commensurate with the perceived risk. The plans are general at the outset, but after contract award, contracting officers shall ensure that the plans are revised to reflect the risks associated with the successful proposal. (See NFS 1846.401).

2.3 The project-specific implementation of the CRM process shall be documented for each project in a Risk Management Plan (RMP). The RMP shall be reviewed by the SAM, approved by the PM and concurred by the SMO Director. The RMP shall be developed, approved and implemented early in project formulation, no later than the mid point of the planned formulation period and prior to any mid formulation review gates imposed by the funding Enterprise (i.e., Office of Space Science Interim Confirmation Review). The RMP is a controlled document and shall be maintained by the PM throughout the project life cycle.

DIRECTIVE NO.	<u>GPG 7120.4</u>
EFFECTIVE DATE:	<u>December 7, 2001</u>
EXPIRATION DATE:	<u>December 7, 2006</u>

The RMP shall include:

- a. Introduction— Specify the project risk objectives and policy toward risk. Explain the purpose, scope, assumptions, constraints, key ground rules, and policy pertaining to the project CRM process.
- b. Overview of process—Provide an overview of the CRM process and information flow; describe how the CRM process integrates and relates to other project management and system engineering activities. Include general risk mitigation strategies to be employed throughout project life cycle.
- c. Organization—Show the organization, roles, and responsibilities of program, project, customer, and supplier key personnel with regard to CRM. Document how team members will be trained in the application of CRM methodology.
- d. Process details—Provide the CRM process details and related procedures, methods, tools, and metrics. Include here, or in an appendix, the specific methodologies to be used for risk identification, analysis, planning, tracking, and controlling. Include the process to be used for continual assessment of the project risk profile. Describe how risk information will be communicated both internally to the project staff and throughout the NASA management chain.
- e. Documentation of risks—Specify the format and data elements that will comprise the project Risk List, how configuration control will be applied, and how the list will be used and updated. Tell how team members will be able to access the current list at any time. Include in the RMP the initial set of identified risks and the action plan (for research, acceptance, tracking, or mitigation) for each risk.

The SMO website: <http://smo.gsfc.nasa.gov> contains CRM training information, and other sample RMP's, information on CRM techniques and tools.

2.4 The PM shall provide CRM training early in project formulation to the project team, including major partners and suppliers, as defined in the RMP. Training in CRM is available from the SMO. PM's and other senior systems management personnel should receive advanced training in risk management. The SMO and Headquarters Office of Safety and Mission Assurance are sources of advanced training in risk management.

2.5 A Failure Modes and Effects Analysis (FMEA) shall be performed early in the design phase to identify system design problems (flight and ground, hardware and software). As additional design information becomes available, the FMEA shall be refined. Failure modes shall be assessed at the component ("box") interface level. Each failure mode shall be assessed for the effect at that level of analysis, the next higher level and upward. The failure mode shall be assigned a severity category based on the most severe effect caused by a failure. All mission phases (e.g., launch, deployment, on-orbit operation, disposal) shall be addressed in the analysis.

Severity categories shall be determined in accordance with following table:

FEMA SEVERITY CATEGORIES

Category	Severity	Description
1	Catastrophic	Failure modes that could result in serious injury, loss of life (flight or ground personnel), or loss of launch vehicle.
1R		Failure modes of identical or equivalent redundant hardware items that, if all failed, could result in category 1 effects.
1S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Severity Category 1 consequences.
2	Critical	Failure modes that could result in loss of one or more mission objectives as defined by the GSFC project office.
2R		Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed.
3	Significant	Failure modes that could cause degradation to mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

Failure modes resulting in Severity Categories 1, 1R, 1S or 2 shall be analyzed at a greater depth, to the single parts, if necessary, to identify the cause of failure. Results of the FMEA shall be used to evaluate the design relative to requirements (e.g., no single instrument failure will prevent removal of power from the instrument). Identified discrepancies shall be evaluated by the MSE, or equivalent, and design groups for assessment of the need for corrective action. The FMEA shall analyze redundancies to ensure that redundant paths are isolated or protected such that any single failure that causes the loss of a functional path will not affect the other functional path(s) or the capability to switch operation to that redundant path.

All failure modes that are assigned to Severity Categories 1, 1R, 1S, and 2, shall be itemized on a Critical Items List (CIL) and maintained with the FMEA report. Rationale for retaining the items shall be included on the CIL. The FMEA and CIL shall be documented and reported in accordance with the RMP.

2.6 Fault Tree Analyses (FTA) shall be performed to address both mission failures and degraded modes of operation. Beginning with each undesired state (mission failure or degraded mission), the fault tree will be expanded to include all credible combinations of events/faults and environments that could

lead to that undesired state. Component hardware/software failures, external hardware/software failures, and human factors will be considered in the analysis. The fault tree in itself is not a quantitative model, but can be combined with quantitative data as part of the Probabilistic Risk Assessment (PRA). The FTA shall be used to evaluate possible system engineering changes that could eliminate or reduce potential failure paths. In particular, an FTA shall be used to identify and develop required operational contingency plans.

2.7 Comparative numerical reliability assessments and/or reliability predictions, such as Probabilistic Risk Assessment (PRA), should be employed to:

- a. Evaluate alternative design concepts, redundancy and cross-strapping approaches, and part substitutions
- b. Identify the elements of the design that are the greatest detractors of system reliability
- c. Identify those potential mission limiting elements and components that will require special attention in part selection, testing, environmental isolation, and/or special operations
- d. Assist in evaluating the ability of the design to achieve the mission life requirement and other reliability goals and requirements as applicable
- e. Evaluate the impact of proposed engineering change and waiver requests on reliability

The RMP shall document the PM's decision on utilizing PRA and similar techniques in the project systems engineering process.

2.8 The results of FMEA's, FTA's and any numerical reliability assessments or predictions shall be reported at system-level critical milestone reviews. The presentations shall include descriptions of how the analysis was used to perform design trade-offs and how the results were taken into consideration when making design or risk management decisions.

2.9 The PM shall maintain a Risk List throughout the project life cycle, along with programmatic impacts. The list should indicate which risks have the highest probability, which have the highest consequences, and which risks represent the greatest risk to mission success. The list should also identify actions being taken to address each specific risk. The Risk List is a controlled document.

2.10 Risk status shall be communicated on a regular basis to the entire project team and customers. Risk status shall be communicated to the PMC through the Monthly Status Reviews.

2.11 For each primary risk (those having both high probability and high impact/severity), the program/project shall develop and maintain the following in the risk sections of the Program/Project Plans and, as appropriate, in the Program Commitment Agreement:

- a. Description of the risk, including primary causes and contributors, actions embedded in the program/project to date to reduce or control it, and information collected for tracking purposes.

DIRECTIVE NO.	<u>GPG 7120.4</u>
EFFECTIVE DATE:	<u>December 7, 2001</u>
EXPIRATION DATE:	<u>December 7, 2006</u>

Page 9 of 10

- b. Primary consequences, should the undesired event occur.
- c. Estimate of the probability (qualitative or quantitative) of occurrence together with the uncertainty of the estimate. The probability of occurrence should take into account the effectiveness of any implemented risk mitigation measures.
- d. Potential additional mitigation measures, including a cost comparison, which addresses the probability of occurrence multiplied by the cost of occurrence versus the cost of risk mitigation.
- e. Characterization of the risk as “acceptable” or unacceptable’ with supporting rationale. Characterization of a primary risk as “acceptable” shall be supported by the rationale, with the concurrence of the GPMC, that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

DIRECTIVE NO. GPG 7120.4
EFFECTIVE DATE: December 7, 2001
EXPIRATION DATE: December 7, 2006

CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes
Baseline	12/07/01	Initial Release