NASA Space Safety Standards and Procedures for Human Rating Requirements

Dr. C. Herbert Shivers, PhD, PE, CSP, Deputy Director, Safety and Mission Assurance Directorate, Marshall Space Flight Center, NASA.

Abstract

The National Aeronautics and Space Administration of the United States of America (NASA) has arguably led this planet in space exploration and certainly has been one of two major leaders in those endeavors. NASA governance is institutionalized and managed in a series documents arranged in a hierarchy and flowing down to the work levels. A document tree of NASA's documentation in its totality would likely overwhelm and not be very informative. Taken in segments related to the various business topics and focusing in those segments, however, provides a logical and understandable relationship and flow of requirements and processes. That is the nature of this chapter, a selection of NASA documentation pertaining to space exploration and a description of how those documents together form the plan by which NASA business for space exploration is conducted.

Information presented herein is taken from NASA publications and is available publicly and no information herein is protected by copyright or security regulations. While NASA documents are the source of information presented herein, any and all views expressed herein and any misrepresentations of NASA data that may occur herein are those of the author and should not be considered NASA official positions or statements, nor should NASA endorsement of anything presented in this work be assumed.

Introduction

This chapter identifies the standards and requirements NASA uses for major programs including some detailed explanation for the Space Shuttle Program. Certainly, the International Space Station and Constellation are the two other large programs of NASA, but including the same level of detail herein for those major programs as well as for major scientific endeavors being conducted via other organizations within the Agency, would likely be minimally instructive compared with the ease by which can obtain relevant information via simple internet searches. To list the documents exhaustively would be tedious and not helpful, but a description of the flow of requirements and identification of the major policy and requirements documents and their tiered relationship to lower level programs along with general pointers to detailed specific standards and requirements might be useful and will be provided. In addition a top level document tree for the Constellation Program is included for illustrative purposes for the planned future work of the Agency in Space Exploration, as is a simple illustration flow down of requirements for a non-crewed science mission launched on an expendable launch vehicle. Some discussion of the NASA Human Ratings process is also included.

NASA Top Level Documentation

Where to start is as challenging as is the enumeration of the multitude of documents, but beginning with NASA's governance policy is as likely a good start as any other. It is from this document that much of the roles and responsibilities are authorized and enumerated. NASA governance is described in NASA Policy Directive - NPD 1000.0, "Strategic Management and Governance Handbook," which is a responsibility of the NASA Administrator's Office. This NPD sets forth NASA's governance framework—principles and structures through which the Agency manages mission, roles, and responsibilities; and describes NASA's strategic management system — processes by which the Agency manages strategy and its implementation through planning, performance, and results. In addition, as a United States Federal Agency, NASA has a public responsibility prescribed in law. "NASA must meet the intent of the National Aeronautics and Space Act of 1958, which established the Agency for the purpose of expanding human knowledge in aeronautical and space activities for the benefit of all humankind. NPD 1000.0A conveys NASA's strategic approach to achieving the Agency's Mission (1)."

In NPD 1000.0, one finds reference to other top level Agency documents pertaining to strategic management and to organization. One also finds a description of the NASA core values, NASA's governance principles, and the strategic management system that defines how the Agency establishes and conducts its missions. NASA's governance provides a check and balance system providing separate and specific authority to programs and institutional entities as they pursue the common goal of mission safety and success. Technical Authority (TA) is a particular item of interest and is delineated separately from programmatic authority as institutional authority feeding into the Administrator. The programs hold certain authorities of risk acceptance and decision making while Institutional TA is provided via Center Directors, Mission Support Authority, Engineering TA, Safety and Mission Assurance TA, and Health and Medical TA. Each of these TA entities has a specific realm of authority that provides the checks and balances of Agency decision making in executing missions. Authorities are exercised in review processes, requirements tailoring, dissenting opinions, etc. Proper implementation of the tenets in NPD 1000.0 demands a proper balance of authority, responsibility and accountability, all of which are described in the NPD.

Perhaps the most useful of NASA's technical guidance documents to provide understanding of program and project execution is NPR 7120.5D, "NASA Program and Project Management Processes and Requirements," which establishes the requirements by which NASA will formulate and implement space flight programs and projects, consistent with the governance model contained in the NASA Strategic Management and Governance Handbook (NPD 1000.0). Figure 1 shows the hierarchy of NASA programmatic requirements. Figure 2 shows the document hierarchy and flowdown methodology.

Direction	Content	Governing Document	Approver	Originator
Needs, Goals, Objectives	Agency strategic direction based on higher-level direction	Strategic Plan and Strategic Planning Guidance	Administrator	Support Organizations
Agency Requirements	Structure, relationships, principles governing design and evolution of cross-Agency/Mission Directorate systems linked in accomplishing Agency needs, goals, and objectives	Architectural Control Document (ACD)	Administrator	Host MDAA with Inputs from Other Affected MDAAs
Mission Directorate Requirements	High-level requirements levied on a Program to carry out strategic and architectural direction including programmatic direction for initiating specific projects	Program Commitment Agreement (PCA)	AA	MDAA
Program Requirements	Detailed requirements levied on a Program to implement the PCA and high-level programmatic requirements allocated from the Program to its projects	Program Plan	MDAA	Program Manager
Project Requirements	Detailed requirements levied on a Project to implement the Program Plan and flow-down programmatic requirements allocated from the Program to the Project	Project Plan	Program Manager	Project Manager
System Requirements	Detailed requirements allocated from the Project to the next lower level of the Project	System Requirements Documentation	Project Manager	Responsible System Lead

MDAA = Mission Directorate Associate Administrator
AA = NASA Associate Administrator

Figure 1 – NASA Programmatic Requirements Hierarchy, taken from NPR 7120.5D, "NASA Program and Project Management Processes and Requirements."

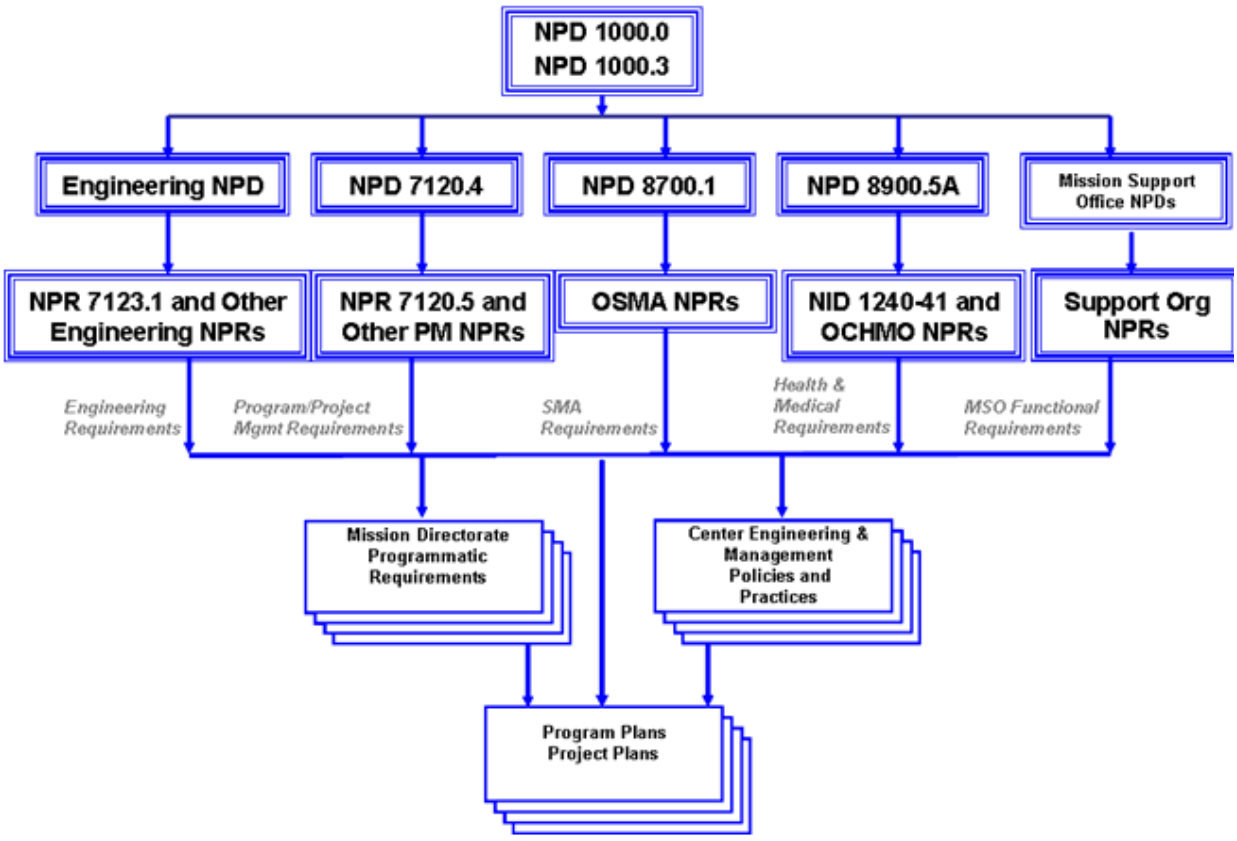


Figure 2 – Program/Project Management Document Hierarchy, taken from NPR 7120.5D, "NASA Program and Project Management Processes and Requirements."

Also useful to understanding the details of programmatic execution is NPR 7123.1, "Systems Engineering Procedural Requirements" which clearly articulates and establishes the requirements on the implementing organization for performing, supporting, and evaluating systems engineering. Systems engineering is a logical systems approach performed by multidisciplinary teams to engineer and integrate NASA's systems to ensure NASA products meet customers' needs. Implementation of this systems approach enhances NASA's core engineering, management, and scientific capabilities and processes to ensure safety and mission success, increase performance, and reduce cost. This systems approach is applied to all elements of a system and all hierarchical levels of a system over the complete project life cycle (2).

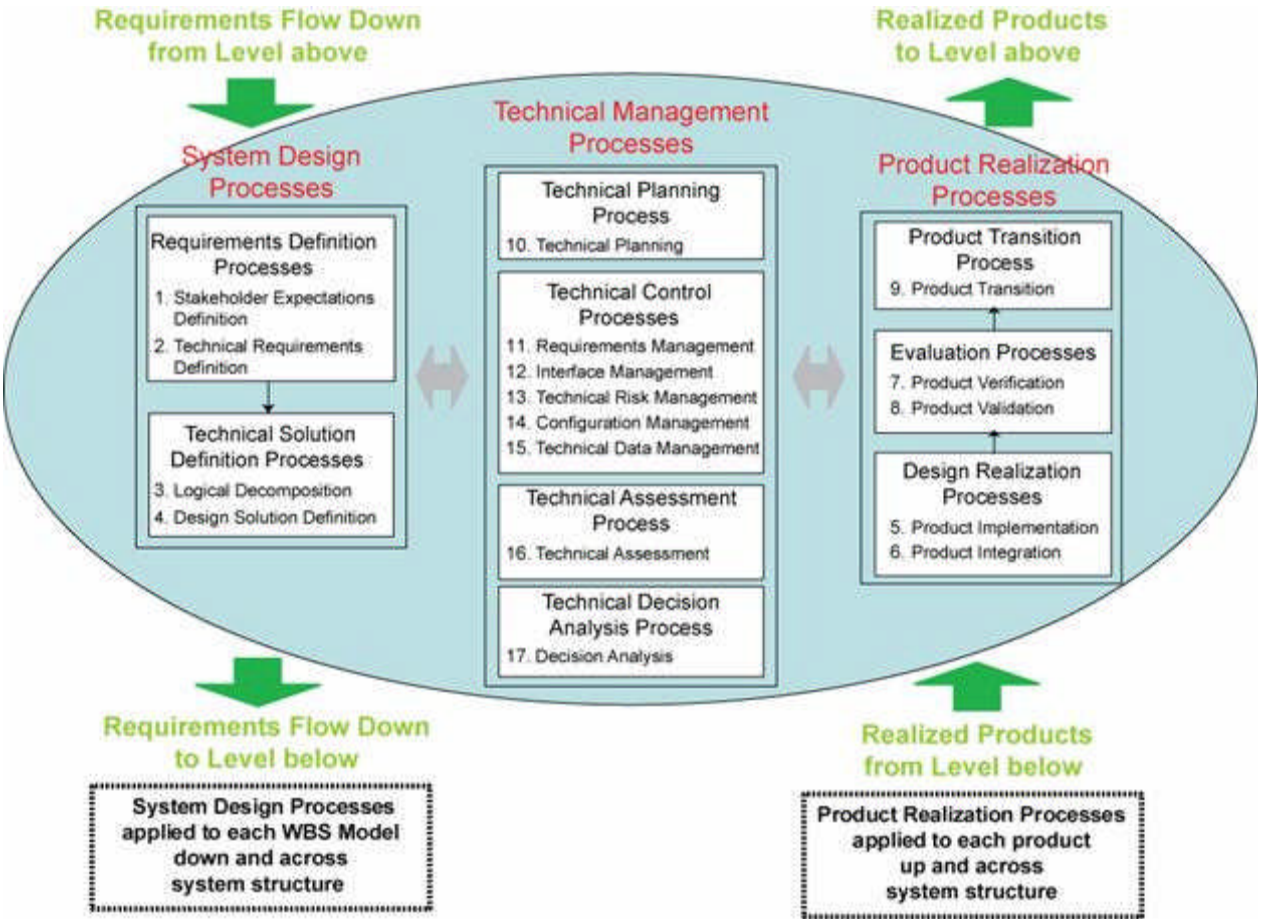


Figure 3 – The Systems Engineering Engine, taken from NPR 7123.1, "Systems Engineering Procedural Requirements"

Another useful illustration from NPR 7123.1, "Systems Engineering Procedural Requirements," is the logical decomposition process shown in Figure 4. The process is used to improve

understanding of the defined technical requirements and the relationships among the requirements (e.g., functional, behavioral, and temporal) and to transform the defined set of technical requirements into a set of logical decomposition models and their associated set of derived technical requirements for input to the design solution definition process.

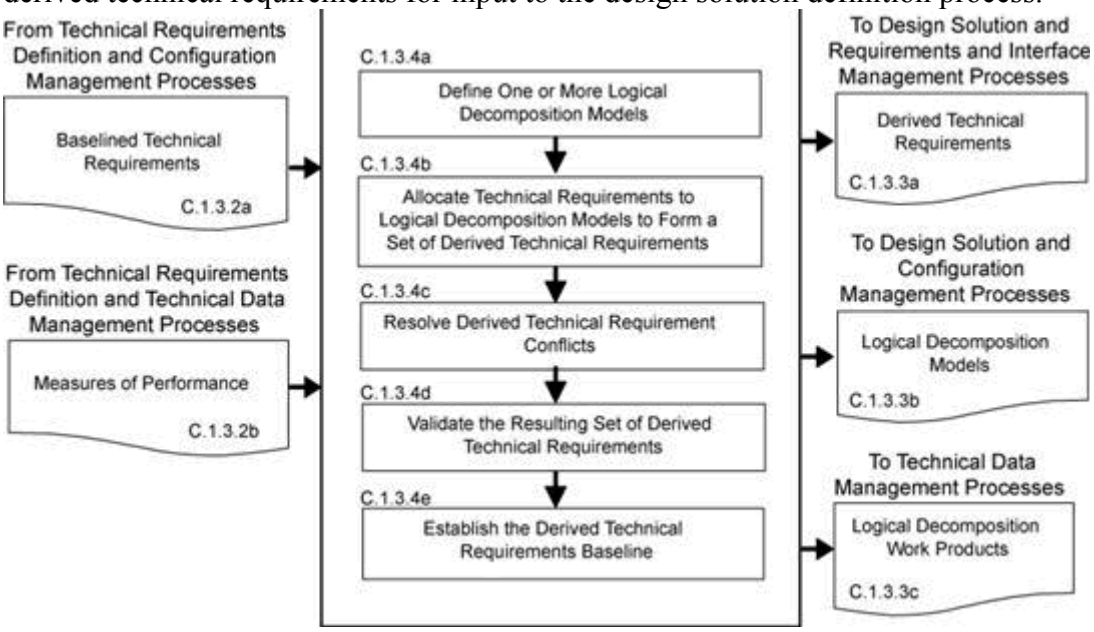


Figure 4 – Logical Decomposition Process

NASA Top Level Safety Standards and Requirements

The NASA Office of Safety and Mission Assurance is responsible for , among others, NPD 8700.1E, "NASA Policy for Safety and Mission Success," which provides top level policy and responsibilities, and NPR 8715.3 General Safety Program Requirements, which provides the top level safety requirements for all Agency activities. "This NASA Procedural Requirements (NPR) provides the basis for the NASA Safety Program and serves as a general framework to structure more specific and detailed requirements for NASA Headquarters, Programs, and Centers (3)." The document is not a standalone document, but is used in conjunction with the references contained within the document. That reference section is an exhaustive bibliography of NASA's safety documentation in a broad sense. Thirty one documents are referred in the "Authority" section and ninety nine are included in the "Applicable Documents" section.

Within those references are the Federal Laws and Directives with which NASA must comply including those specific to activities in space exploration. Some items of particular interest to this subject are (the original numbering from the parent document is intentional):

j. NPD 8700.1, "NASA Policy for Safety and Mission Success."
k. NPD 8700.3, "Safety and Mission Assurance (SMA) Policy for Spacecraft, Instruments, and Launch Services."
m. NPD 8710.3, "NASA Policy for Limiting Orbital Debris Generation."
n. NPD 8710.5, "NASA Safety Policy for Pressure Vessels and Pressurized Systems."

o. NPR 8715.7, “Expendable Launch Vehicle Payload Safety Program.”
p. NPD 8720.1, “NASA Reliability and Maintainability (R&M) Program Policy.”
q. NPD 8730.5, “NASA Quality Assurance Program Policy.”
aa. NPR 7120.5, “NASA Program and Project Management Processes and Requirements.”
ab. NPR 7120.6, “Lessons Learned Process.”
ac. NPR 7123.1, “Systems Engineering Procedural Requirements.”
ad. NPR 7150.2, “NASA Software Engineering Requirements.”
af. NPR 8000.4, “Risk Management Procedural Requirements.”
ai. NPR 8705.2, “Human-Rating Requirements for Space Systems.”
aj. NPR 8705.4, “Risk Classification for NASA Payloads.”
ak. NPR 8705.5, “Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects.”
al. NPR 8705.6, “Safety and Mission Assurance Audits, Reviews, and Assessments.”
ao. NPR 8715.5, “Range Safety Program.”
ap. NPR 8715.6, “NASA Procedural Requirements for Limiting Orbital Debris.”
ar. NASA-STD-8709.2, “NASA Safety and Mission Assurance Roles and Responsibilities for Expendable Launch Vehicle Services.”
at. NASA-STD-8719.8, “Expendable Launch Vehicle Payload Safety Review Process Standard.”
aw. NASA-STD-8719.13, “Software Safety Standard.”
ax. NASA-STD-8739.8, “Software Assurance Standard.”
ba. NSS 1740.14, “Guidelines and Assessment Procedures for Limiting Orbital Debris.”
bb. MIL-STD-882, “Standard Practice for Safety Systems.”
bd. SSP 50021, “Safety Requirements Document.”
bi. “Wallops Flight Facility Range Safety Manual.”
bj. AFSPCMAN 91710, “Licensing and Safety Requirements for Launch.”
cp. “Eastern and Western Range (EWR) 127-1, “Range Safety Requirements.”
cq. NASA SP 8013, “NASA Micrometeoroid Environment Model [Near Earth to Lunar Surface].”
cr. NASA SP 8038, “Micrometeoroid Environment Model [Interplanetary and Planetary].”
cs. SSP 30425, “Space Station Program Natural Environment Definition for Design.”
ct. NASA TM 4527, “Natural Orbital Environment Guidelines for Use in Aerospace Vehicle Development.”
cu. "Meteoroid Engineering Model (MEM): A Meteoroid Model for the Inner Solar System," H. McNamara, R. Suggs, B. Kauffman, J. Jones, W. Cooke, and S. Smith: 2004, Earth Moon and Planets, 95, 123-139.

NASA uses these and other requirements to meet its stated goal: “NASA's goal is to maintain a world-class safety program based on management and employee commitment and involvement; system and worksite safety and risk assessment; hazard and risk prevention, mitigation, and control; and safety and health training (4).”

NASA’s Safety and Mission Assurance Requirements Tree is included as Appendix A. In this figure, one sees the relationship of the top level documents and the flow to S&MA disciplines and programs and projects. In addition reference is made to the NASA Technical Standards Program and to the NASA Directives System where the documents listed above and others may be found. Again, a simple internet search will yield links to these systems or documents, but

being designed primarily for the use of NASA employees, there are specific requirements for system access, left to the reader to explore.

NASA Human Ratings Process

Of particular interest are the Human Rating Requirements imposed by NASA on select systems. Many NASA systems require "Human Rating." Systems requiring Human Rating must implement additional processes, procedures, and requirements necessary to produce human-rated space systems that protect the safety of crew members and passengers on NASA space missions. Human-rated systems accommodate human needs, effectively utilize human capabilities, control hazards and manage safety risk associated with human spaceflight, and provide, to the maximum extent practical, the capability to safely recover the crew from hazardous situations. Human-rating is an integral part of all program activities throughout the life cycle of the system, including design and development; test and verification; program management and control; flight readiness certification; mission operations; sustaining engineering; maintenance, upgrades, and disposal.

The Human-Rating Certification is granted to the crewed space system but the certification process and requirements affect functions and elements of other mission systems, such as control centers, launch pads, and communication systems. The types of crewed space systems that require a Human-Rating Certification include, but are not limited to, spacecraft and their launch vehicles, planetary bases and other planetary surface mobility systems that provide life support functions, and Extravehicular Activity (EVA) suits. A crewed space system consists of all the system elements that are occupied by the crew during the mission and provide life support functions for the crew. The crewed space system also includes all system elements that are physically attached to the crewed-occupied element during the mission, while the crew is in the vehicle/system.

Verification of program compliance with the Human Ratings requirements is performed in conjunction with selected milestone reviews (System Requirements Review (SRR), System Definition Review (SDR), Preliminary Design Review (PDR), Critical Design Review (CDR), System Integration Review (SIR) and the Operational Readiness Review (ORR)) conducted in accordance with the requirements of NPR 7120.5, "NASA Space Flight Program and Project Management Requirements," and NPR 7123.1, "NASA Systems Engineering Processes and Requirements." NPR 8705.2, "Human-Rating Requirements for Space Systems," specifies development of products that are reviewed at each of the selected milestone reviews. The adequacy of those products and the acceptability of progress toward Human-Rating Certification are used to verify compliance. In addition, the Human Rating requirements and processes are subject to audit and assessment in accordance with the requirements contained within NPR 8705.6, "Safety and Mission Assurance Audits, Reviews, and Assessments."

NPR 8705.2, "Human-Rating Requirements for Space Systems," also defines and delineates specific responsibilities for Human Rating including overall authority assigned to the NASA Associate Administrator and assurance of implementation assigned to the Chief, Safety and

Mission Assurance, and the NASA Chief Engineer as Technical Authorities within their realms of responsibility. Additional responsibilities and authorities are described as appropriate.

The Human-Rating Certification Process is linked to five major program milestones: System Requirements Review, System Definition Review, Preliminary Design Review, Critical Design Review, and Operational Readiness Review. The program's compliance with the human-rating requirements and the contents of the Human Rating Certification Package are endorsed and approved by all three Technical Authorities (Safety, Engineering, and Health and Medical) at each of the five milestones. Since it is not the intent of this article to restate the documented requirements and processes required for human rating, a summary of major certification elements from the NPR 8705.2 is hereby provided:
a. The definition of reference missions for certification.
b. The incorporation of system capabilities to implement crew survival strategies for each phase of the reference missions.
c. The implementation of capabilities from the applicable technical requirements.
d. The utilization of safety analyses to influence system development and design.
e. The integration of the human into the system and human error management.
f. The verification, validation, and testing of critical system performance.
g. The flight test program and test objectives.
h. The system configuration management and related maintenance of the Human-Rating Certification.

"A human-rated system accommodates human needs, effectively utilizes human capabilities, controls hazards with sufficient certainty to be considered safe for human operations, and provides, to the maximum extent practical, the capability to safely recover the crew from hazardous situations. Human-rating consists of three fundamental tenets: (1) Human-rating is the process of designing, evaluating, and assuring that the total system can safely conduct the required human missions. (2)Human-rating includes the incorporation of design features and capabilities that accommodate human interaction with the system to enhance overall safety and mission success. (3) Human-rating includes the incorporation of design features and capabilities to enable safe recovery of the crew from hazardous situations. Human-rating is an integral part of all program activities throughout the life cycle of the system, including design and development; test and verification; program management and control; flight readiness certification; mission operations; sustaining engineering; maintenance/upgrades; and disposal (5)."

Specific requirements, including specific technical requirements that are described in Chapter 3 of the NPR 8705.2 are available for review by the interested reader.

Flowdown Methodology

NASA requirements are designated by level and flow down to lower work levels gaining more specificity as the levels change. All programs and projects are required to specifically identify those requirements that are applicable and track and verify status of completion in verification

plans before mission execution. In conjunction with the Technical Authorities, agreement is reached for the complement of requirements for specific projects. Generally the levels can be described as follows:

- Level 0 – Top Level Agency Requirements controlled by the Administrator and Associate Administrators
- Level 1 Requirements - Mission Drivers controlled by a NASA Mission Directorate and serve as the basis for mission assessment during development. These are NASA requirements and standards - latest versions apply
- Level 2 Requirements - System/Segment (Mission Requirements Document– to be baselined at System Requirements Review)
- Level 3 Requirements - Element (Instruments, Spacecraft, etc.)
- Level 4 Requirements - Subsystem (Instrument Subsystem, Spacecraft Subsystem, etc.)
- Level 5 Requirements - Component (Instrument Component, Spacecraft Component, etc.)

Space Shuttle Program

The Space Shuttle Program (SSP) Manager documents and controls program requirements in Volume I through XVIII of NSTS 07700, "Program Definition and Requirements Document (6)." This document is supported by more than 225 subordinate NSTS documents, more than 400 applicable documents and thousands of project and element level documents. Specific content topics of NSTS 07700 are structured as shown in Appendix B. In addition there is a Shuttle Master Verification Plan supported by subordinate verification plans, Shuttle System Interface Control Documents, Payload Interface Control Documents, and Operations and Maintenance Documents. NSTS 08171, "Operations and Maintenance Requirements and Specifications Document (OMRSD)" is the location for on-line operations and maintenance tasks to support Space Shuttle turnaround. NSTS 08151, "Intermediate and Depot Maintenance Requirements Document (IDMRD)" is the location for off-line operations and maintenance tasks in support of Space Shuttle turnaround. The Certification of Flight Readiness (CoFR) process, documented in NSTS 08117, "Space Shuttle Requirements and Procedures for Certification of Flight Readiness," constitutes the main part of the SSP risk management review process. NSTS 16007, "Shuttle Launch Commit Criteria and Background Document," is the Space Shuttle Program baseline document that provides the launch support system and the launch team with the Shuttle launch commit criteria and background information.

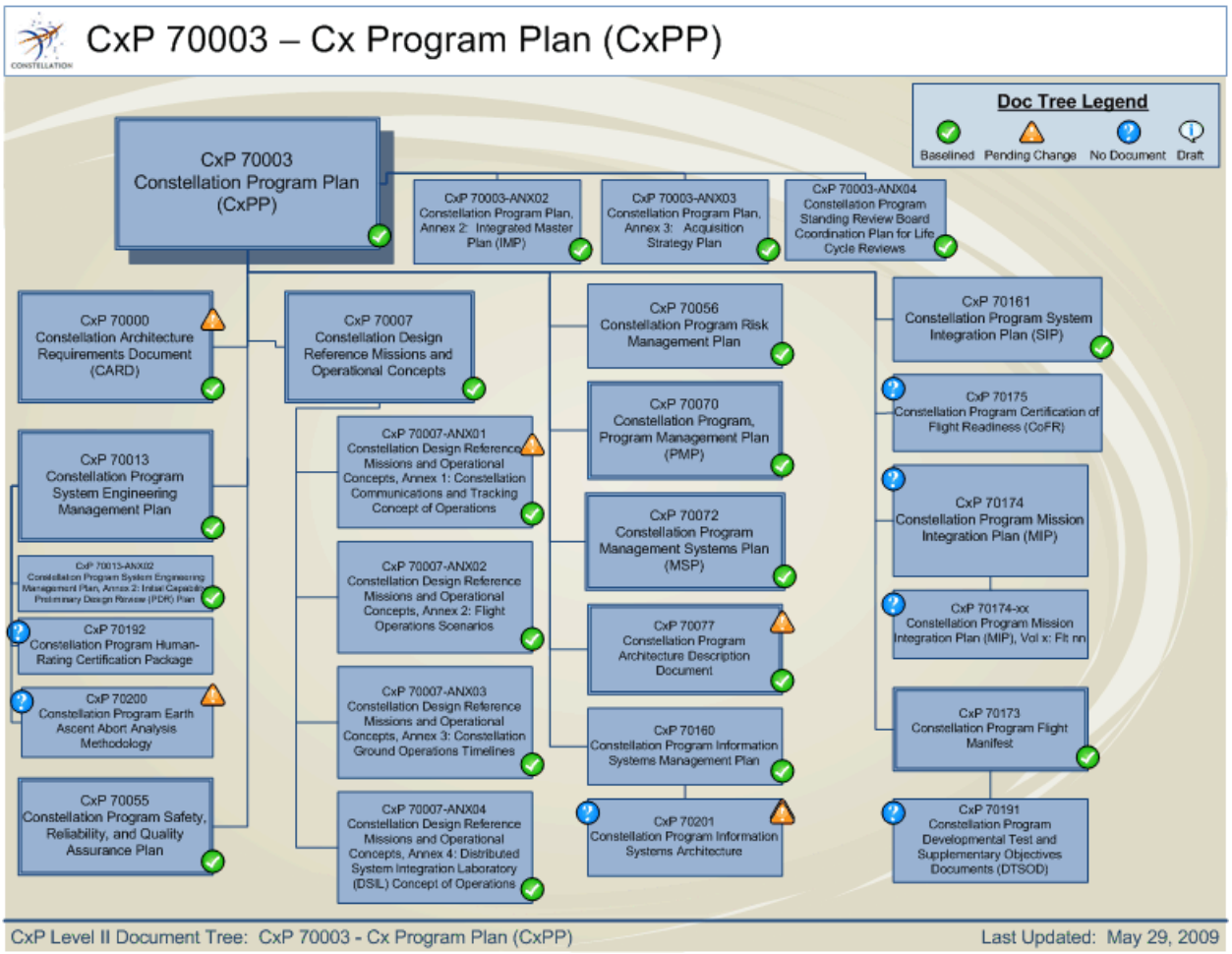
NSTS 5300.4(1D-2), "Space Shuttle Safety, Reliability, Maintainability and Quality Provisions for the Space Shuttle Program," establishes common safety, reliability, maintainability and quality provisions for the Space Shuttle Program. NSTS 22206, "Requirements for Preparation and Approval of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)," provides detailed instructions for the preparation of Failure Modes and Effects Analyses (FMEAs) and Critical Items Lists (CILs). NSTS 22254, "Methodology for Conduct of Space Shuttle Program Hazard Analyses," provides the methodology required for the preparation of SSP hazard analyses, hazard reports, safety analysis reports, and Management Safety Assessments. NSTS 08209, "Shuttle Systems Design Criteria," is a seven volume set of design

criteria and performance requirements. The Shuttle Operational Data Book, "NSTS 08934 (JSC 08934)," also a seven volume set, is the single authoritative source of properly validated data, which most accurately and completely describe the Shuttle operational performance capabilities and limitations. Other critical Shuttle Program documents include:

- NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System"
- NSTS 08080-1, "Manned Spacecraft Criteria and Standards"
- NSTS 12820, "STS Operational Flight Rules"
- NSTS 08126, "Problem Reporting and Corrective Action (PRACA) System Requirements"
- NSTS 17462, "Flight Requirements Document (FRD) and other payload/flight related documents"
- JSC 17481A, "JSC Safety Requirements Document for Space Shuttle Flight Equipment"

Space Exploration (Constellation) Program

Constellation is the program NASA has developed to meet the United States' Vision for Space Exploration. The Program includes developing new launch and crew vehicles for journeys to the Earth's moon, to Mars, and beyond. The Constellation Program Document Tree follows:



A Typical Non-Crewed Mission Launched on an Expendable Launch Vehicle

Program Level Requirements for the typical science program project launched on an ELV:

Level 1 Requirements - Mission Drivers
Program Level 1 Requirements - baselined after Key Decision Point, KDP-A

- Highest unique requirements for the project
- Controlled by Science Mission Directorate, documented in the Program Plan Program Level Requirements Appendix
- Imposed for the development and operation of the project
- Serve as the basis for mission assessment during development
- Provide the baseline for determination of science mission success
  – NASA requirements and standards - latest versions apply

• Level 2 Requirements - System/Segment (project Mission Requirements Document)
  – Baseline at Systems Requirements Review

• Level 3 Requirements - Element (Instruments, Spacecraft, etc.)

• Level 4 Requirements - Subsystem (Instrument Subsystem, Spacecraft Subsystem, etc.)

• Level 5 Requirements - Component (Instrument Component, Spacecraft Component)

Conclusion

Protecting the health and safety of humans involved in or exposed to space activities, specifically the public, crew, passengers, and ground personnel is NASA policy. The policy is implemented through the application of NASA directives and standards through a rigorous process of identification, allocation and verification. As the NASA activities are carried out, general and specific requirements are identified and allocated as appropriate to the programs and projects and verified to have been met before mission execution. The process is exhaustive and deliberate to ensure that safety and mission success are achieved. This article is intended to provide a glimpse into the intricate inner workings of that process.

REFERENCES

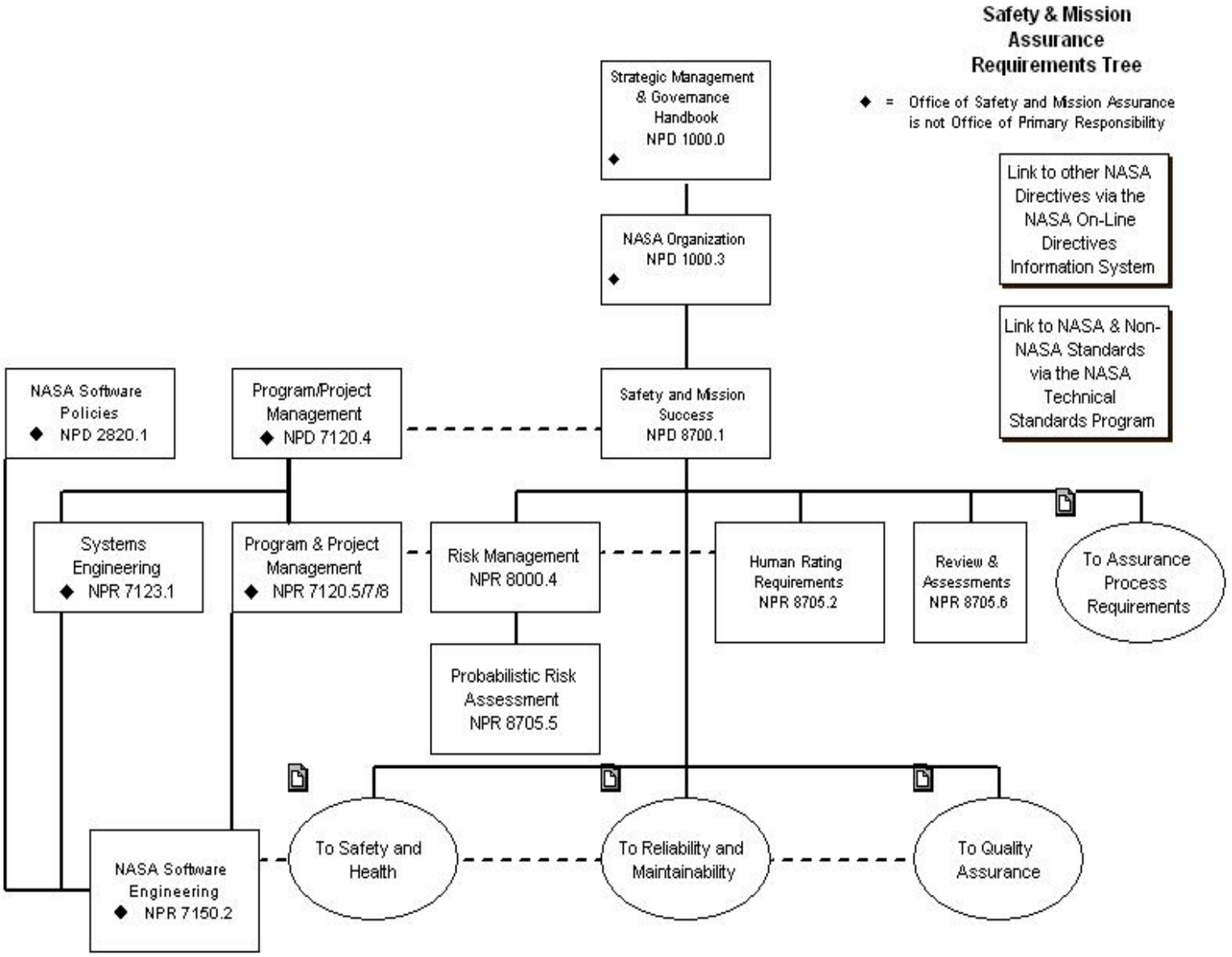
1. NPD 1000.0, Strategic Management and Governance Handbook.
2. NPR 7123.1, Systems Engineering Procedural Requirements.
3. NPR 8715.3 General Safety Program Requirements.
4. NPR 8715.3 General Safety Program Requirements, p 17.
5. NPR 8705.2, Human-Rating Requirements for Space Systems.
6. NSTS 07700, Program Definition and Requirements Document.

Appendix A

NASA Safety and Mission Assurance Requirements Tree

Appendix A

NASA Safety and Mission Assurance Requirements Tree



APPENDIX B

NSTS 07700

Contents

APPENDIX B

NSTS 07700 Contents

NSTS 07700 Documents (Current Issue)	Document Title
Volume I	Program Description and Requirements Baseline
Volume II, Book 2	Program Structure and Responsibilities, Book 2 - Space Shuttle Program Directives
Volume II, Book 3	Program Structure and Responsibilities, Book 3 - Space Shuttle Program Interface Agreements
Volume III	Flight Definition and Requirements Directive
Volume IV, Book 1	Configuration Management Requirements, Book 1 - Requirements
Volume IV, Book 2	Configuration Management Requirements, Book 2 - Configuration Deviations/Waivers
Volume V	Information Management Requirements
Volume VI	Flight Support Equipment (FSE) Management
Volume VIII	Operations
Volume IX	Ground Systems Integration and Operations
Volume X, Book 1	Flight and Ground System Specification - Book 1, Requirements (Section 1.0 - 6.0)
Volume X, Book 2	Flight and Ground System Specification - Book 2, Environment Design, Weight and Performance, and Avionics Events (Apx 10.3 - 10.16)

Volume X, Book 3	Flight and Ground System Specification - Book 3, Requirements for Runways and Navigation Aids (Apx 10.17)
Volume X, Book 4	Flight and Ground System Specification - Book 4, Active Deviations/Waivers
Volume X, Book 6	Flight and Ground System Specification - Book 6, Retired Deviations/Waivers (Apx 10.1)
Volume XI	System Integrity Assurance Program Plan
Volume XII	Program Logistics and Supportability Requirements
Volume XIV	Space Shuttle System Payload Accommodations
Volume XV	Resource Management Policy and Requirements
Volume XVIII, Book 1	Computer Systems and Software Requirements - Book 1, Allocation of Computational Functions
Volume XVIII, Book 2	Computer Systems and Software Requirements - Book 2, Allocation of Simulation Functions
Volume XVIII, Book 3	Computer Systems and Software Requirements - Book 3, Software Management and Control
NSTS 07700-10-MVP-01	Shuttle Master Verification Plan - Volume I, General Approach and Guidelines
NSTS 07700-10-MVP-02	Shuttle Master Verification Plan - Volume II, Combined Element Verification Plan
NSTS 07700-10-MVP-09, Part 1	Shuttle Master Verification Plan - Volume IX, Computer Systems and Software Verification Plan - Part 1, Guidelines and Standards
NSTS 07700-10-MVP-09, Part 2	Shuttle Master Verification Plan - Volume IX, Computer Systems and Software Verification Plan - Part 2, Verification Requirements