Glenn Procedural Requirements

GLPR 7120.5.30

Effective Date: November 3, 2009
Expiration Date: November 3, 2014

COMPLIANCE IS MANDATORY

This Document Is Uncontrolled When Printed.
Validate prior to use at https://knowledgeshare.grc.nasa.gov/bmslibrary

---

Responsible Office: Q/Safety and Mission Assurance Directorate

Space Assurance Requirements w/Change 1 (12/22/09)

TABLE OF CONTENTS

Preface 7
P.1 Purpose 7
P.2 Applicability 7
P.3 Authority 8
P.4 Applicable Documents 8
P.5 Reference Documents 10
P.6 Measurement/Verification 12
P.7 Cancellation 12

Chapter 1. Responsibilities 13
1.1 GRC Management 13
1.2 Project Manager (PM) 13
1.3 Project Chief Engineer (PCE) 13
1.4 Lead Systems Engineer (LSE) 13
1.5 Chief Safety and Mission Assurance Officer (CSO) 13
1.6 System Safety Lead Engineer 14
1.7 Reliability Lead Engineer 14
1.8 Materials and Processes (M&P) Lead Engineer 14

1.9 Quality Assurance (QA) Lead Engineer 15
1.10 Software Assurance (SA) Lead Engineer 15

Chapter 2. Overall Responsibilities 16
2.1 Description of Overall Requirements 16
2.2 Safety and Mission Assurance Plan 16
2.2.1 Use of Deviations 17
2.3 Use of Previously Designed, Fabricated, or Flown Systems 17
2.3.1 Storage Requirements for Suspended Projects 17
2.4 Assurance Status Reports 18
2.5 Contractor Surveillance 19
2.6 GRC Assurance Review Requirements 19
2.7 Mishap Reporting and Investigation 19
2.8 Safety, Health, and Environmental 19

Chapter 3. Design and Verification 21
3.1 General Requirements 21
3.2 Overall Verification Program 21
3.3 Electrical Verification Requirements 22
3.4 Structural and Mechanical Requirements 23
3.4.1 Safety- and Fracture-Critical Structures 23
3.4.2 Structural Loads 24
3.4.3 Factors of Safety 24
3.4.4 Margins of Safety 24
3.4.5 Fracture Control 26
3.4.6 Pressurized Systems 27
3.4.7 Strength Testing 27
3.4.8 Vibroacoustics 28
3.4.9 Shock (Mechanical and Pyro) 33
3.4.10 Mechanical Function 34
3.4.11 Pressure Profile 34
3.4.12 Fastener Integrity 35
3.4.13 Mass Properties 35
3.4.14 Ground Support Equipment 36
3.5 Electromagnetic Compatibility (EMC) Requirements 37
3.5.1 EMC Guidance 37
3.6 Radiation Requirements 38
3.7 Vacuum, Thermal, and Humidity Requirements 39
3.7.1 Compliance With Requirements 39
3.7.2 Testing Levels 39
3.7.3 Description of Applicable Testing 40
3.7.4 Description of Applicable Analysis 40
3.8 Flight System Performance Acceptance Test Requirements 41
3.8.1 Burn-In Tests 41
3.8.2 Mission Simulation Test 41
3.8.3 End-to-End Compatibility Test 41

Chapter 4. System Safety 42

4.1 Introduction ... 42
4.2 System Safety Planning ... 42
4.2.1 System Safety Assurance Reviews ... 42
4.3 Hazards Analysis ... 43
4.4 Failure Tolerance ... 43
4.5 Design for Minimum Risk ... 43
4.6 Internal GRC Review of Safety Products ... 44
4.7 Requirements Applicability ... 44

Chapter 5. EEE and Mechanical Parts Control ... 45
5.1 General Requirements ... 45
5.2 EEE Parts Selection and Screening ... 45
5.2.1 EEE Parts Control Plan ... 45
5.2.2 EEE Parts Selection and Grade ... 45
5.2.3 Flight EEE Parts Qualification ... 46
5.2.4 Flight EEE Parts Screening ... 46
5.2.5 De-rating ... 46
5.2.6 Radiation Hardness ... 47
5.2.7 Corona and Arcing ... 47
5.2.8 Inspection Prior to Assembly ... 49
5.3 Mechanical Parts Selection and Screening ... 49
5.3.1 Mechanical Parts Control Plan ... 49
5.3.2 Inspection Prior to Assembly ... 49
5.4 Procurement of Parts ... 49
5.4.1 Parts Obsolescence and Diminishing Manufacturing Sources ... 49
5.5 Parts Storage Control ... 49
5.6 Parts Age Control ... 49
5.7 Parts Identification List ... 49
5.8 Parts Risk Evaluation ... 50
5.9 Parts Subject to Metal Whisker Growth ... 50

Chapter 6. Materials and Processes Requirements ... 51
6.1 General Requirements ... 51
6.2 Safety and Mission Assurance Plan Specific Requirements ... 52

Chapter 7. Reliability and Probabilistic Risk Assessment ... 53
7.1 Reliability, Availability, and Maintainability ... 53
7.1.1 General Requirements ... 53
7.1.2 Requirement for and Integrated Process ... 53
7.1.3 RAM Management ... 54
7.1.4 RAM Plan ... 54
7.1.5 RAM Data ... 54
7.1.6 RAM Reports Archives ... 55
7.1.7 Reliability and Failure Tolerance ... 55
7.2 Probabilistic Risk Assessment (PRA) ... 55
7.2.1 General Requirements ... 55
7.2.2 Criteria for PRA Decision ... 56
7.2.3 PRA Objectives and Ground Rules ... 56

7.2.4 Application of PRA 56
7.2.5 Requirement for an Integrated Process 56
7.2.6 PRA Management 57
7.2.7 PRA Plan 57

Chapter 8. Quality Assurance Requirements 58
8.1 General Requirements 58
8.2 Quality Assurance Organization 59
8.3 Configuration Management (CM) and Verification 60
8.4 Identification and Traceability 60
8.5 Procurement Requirements 61
8.5.1 Government Source Inspection 61
8.5.2 Receiving Inspection 61
8.6 Control of Fabrication Activities 61
8.6.1 Fabrication and Inspection Requirements 62
8.6.2 Training for Personnel 63
8.6.3 Evaluation and Control of Process Specifications and Procedures 63
8.6.4 Bonded Storage 63
8.6.5 Records of Inspections and Tests 63
8.7 Contamination Control 63
8.7.1 Contamination Control Plan 64
8.8 Electrostatic Discharge Prevention 64
8.9 Nonconformance and Problem Reporting and Control 65
8.9.1 Review Boards 65
8.9.2 Waivers and Deviations 65
8.10 Alert Information 66
8.11 Inspection and Test of Stored Limited-Life Hardware 66
8.12 Metrology 66
8.13 Handling, Preservation, Marking, Packaging, Packing, and Transportation 66
8.13.1 Control of Government Property by Contractors 67
8.14 Configuration Verification 67
8.15 Acceptance of Flight System 67
8.16 Quality Program Audits 68
8.17 Control of Quality Records 68

Chapter 9. Continuous Risk Management 69
9.1 Risk 69
9.2 Introduction 69
9.2.1 Risk Informed Decision Making (RIDM) 69
9.2.2 Continuous Risk Management (CRM) 69
9.2.3 RIDM and CRM 70
9.2.4 Institutional Risks 70
9.3 General Requirements 70
9.4 Initial Risk Management Training 71
9.5 Implementation 71
9.5.1 Identify Risks 71
9.5.2 Analyzing Risks 72

9.5.3 Planning 72
9.5.4 Risk Tracking 73
9.5.5 Risk Control 73
9.5.6 Communication and Documentation 74

Chapter 10. Software Assurance 75
10.1 General Requirements 75
10.1.1 Roles and Responsibilities 75
10.1. 2 Scope of Software Assurance Activities 75
10.2 Software Safety 75
10.3 Software Reliability 76
10.4 Software Configuration Management 76
10.5 Software Nonconformance Reporting and Corrective Action 76
10.6 Software Verification and Validation 76
10.6.1 Software Review 76
10.6.2 Software Inspections 77
10.6.3 Software System Testing 77
10.6.4 Software Audits 77
10.6.5 Software Acceptance 78

Appendix A. Definitions 79

Appendix B. Acronyms 85

Appendix C. Verification Matrix 89

Appendix D. Templates and Forms 94
D.1 Safety and Mission Assurance Plan Template 94
D.2 Certificate of Flight Readiness 111

Appendix E. Internet Resources 113

LIST OF FIGURES

Figure 3.4-1—Vibration Testing of Stowed Hardware for Protoflight Project. 31
Figure 3.4-2—Vibration Testing of Stowed Hardware for Prototype Project. 32

LIST OF TABLES

Table 2-1—Control Plans 17
Table 3.4-1—Executive Summary of NASA-STD-7001 Verification Test Requirements[3] 28
Table 3.4-2—Component Minimum Workmanship Random Vibration Test Levels 29
Table 3.4-3—Example of Weight Contingencies Applied at the Component and Subsystem Level. 36

Change History

Change	Date	Description/Comments
Basic	11/3/09	This document was created to assure the Center's compliance to NPR 7120.5 and NPR 7123.1 and to be used as a tool for the Center's project teams.
1	12/22/09	Administrative change – corrected the Chapter 4 title which was originally supposed to be named "System Safety;" added the change to the TOC as well.

Preface

P.1 Purpose

a. The purpose of this document is to promote the safety and success of space flight programs and projects managed by Glenn Research Center (GRC). This document defines the overall requirements, assurance review, verification, system safety, electrical, electronic, electro-mechanical (EEE) and mechanical parts, materials and processes, reliability and maintainability, quality assurance (QA), continuous risk management, and software assurance (SA) requirements that ***shall*** be followed.

b. The projects in the context of this document are defined as any organized effort with a Space Projects (Code M) assigned project manager (PM). These assignments may range from NPR7120.5-defined programs to subprojects managed through other NASA Centers.

c. This procedure is a combination of Center requirements and project implementation best practices. The Center requirements are identified with "***shall***" statements. All other material is considered guidance that can be tailored per the needs of the project.

P.2 Applicability

a. This Glenn Procedural Requirement (GLPR) applies to GRC, including contractors/service providers to the extent specified in their contracts with NASA.

b. The requirements of this document apply in all modes of project implementation for those deliverables for which GRC is responsible. This includes when the flight system effort is contracted, when the flight system is a shared responsibility of GRC and a partner, as well as projects implemented in an "in-house" mode.

c. This GLPR applies to current and future NASA GRC programs and projects that involve Flight Systems and Ground Support (FS&GS), and Advanced Technology Development (ATD) programs/projects directly funded by FS&GS programs/projects, or ATD programs/projects with outcomes directly tied to space flight mission success and schedule.

d. This GLPR applies to space flight programs/projects performed for non-NASA sponsors.

e. For existing programs and projects, the requirements of this document are applicable to the program/project's current phase as of the effective date of this GLPR and to phases yet to be completed.

f. The requirements of this document are not required on flight systems elements that are produced under the control and requirements of other NASA Centers or other government agencies. However, application of these requirements is at the option of the GRC project on which these elements are manifested.

g. The requirements of this GLPR do not apply to technology readiness levels (TRLs) 1 to 3 devices. However, this document can and should be used as a guideline making NASA GRC a more streamlined and responsive Center for taking technology programs to flight demonstration.

P.3 Authority

a. NPD 8700.1, “NASA Policy for Safety and Mission Success”

b. NPD 8700.3, “Safety and Mission Assurance (SMA) Policy for NASA Spacecraft, Instruments, and Launch Services”

c. NPR7120.5, “NASA Space Flight Program/Project Management Requirements”

d. GLP-QE-8700.3, “GRC Space Product Assurance”

P.4 Applicable Documents

a. AIAA S-111-205, “Qualification and Quality Requirements for Space Solar Cells”

b. AIAA S-112-205, “Qualification and Quality Requirements for Space Solar Panels”

c. ANSI/AIAA S-080, “Space Systems-Metallic Pressure Vessels, Pressurized Structures, and Pressure Components”

d. ANSI/AIAA S-081, “Space Systems-Composite Overwrapped Pressure Vessels (COPV)”

e. ANSI/ESD S20.20, “Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)”

f. ASME Y14.5, “Dimensioning and Tolerancing”

g. IPC-2221, “Generic Standard on Printed Board Design”

h. IPC-2222, “Sectional Design Standard for Rigid Organic Printed Boards”

i. MIL-STD-461E, “Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment”

j. MIL-STD-1540, “Test Requirements for Launch, Upper-Stage, and Space Vehicles”

k. EEE-INST-002, “Instructions for EEE Parts Selection, Screening, Qualification, and Derating”

l. NASA-STD-(I)-5005, “Standard for the Design and Fabrication of Ground Support Equipment”

m. NASA-STD-4003, “Electrical Bonding for NASA Launch Vehicles, Spacecraft, Payloads, and Flight Equipment”

n. NASA-STD-4005, “Low Earth Orbit Spacecraft Charging Design Standard”

o. NASA-STD-5001, “Structural Design and Test Factors of Safety for Space-Flight Hardware”

p. NASA-STD-5002, “Load Analyses of Spacecraft and Payloads”

q. NASA-STD-5003, “Fracture Control Requirements for Payloads Using the Space Shuttle”

r. NASA-STD-5007, “General Fracture Control Requirements for Manned Space-Flight Systems”

s. NASA-STD-5017, “Design and Development Requirements for Mechanisms”

t. NASA-STD-5019, “Fracture Control Requirements for Spaceflight Hardware”

u. NASA-STD-6016, “Standard Materials and Processes Requirements for Spacecraft”

v. NASA-STD-7001, “Payload Vibroacoustic Test Criteria”

w. NASA-STD-7002, “Payload Test Requirements”

x. NASA-STD-7003, “Pyroshock Test Criteria”

y. NASA-STD-8719.13, “NASA Software Safety Standard”

z. NASA-STD-8739.1, “Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies”

aa. NASA-STD-8739.2, “Workmanship Standard for Surface Mount Technology”

ab. NASA-STD-8739.3, “Soldered Electrical Connections”

ac. NASA-STD-8739.4’ “Interconnecting Cables, Harnesses, and Wiring”

ad. NASA-STD-8739.5, “Fiber Optics Terminations, Cable Assemblies, and Installation”

ae. NASA-STD-8739.8, “NASA Software Assurance Standard”

af. NPSL, “NASA Parts Selection List”

ag. KHB 1700.7, “Space Shuttle Payload Ground Safety Handbook”

ah. NPD 1280.1, “NASA Management System Policy”

ai. NPD 1440.6, “NASA Records Management”

aj. NPD 8730.1, “Metrology and Calibration”

ak. NPD 8730.2, “NASA Parts Policy”

al. NPD 8730.5, “NASA Quality Assurance Program Policy”

am. NPR 1441.1, “NASA Records Retention Schedules”

an. NPR 7150.2, “NASA Software Engineering Requirements”

ao. NPR 8000.4, “Risk Management Procedural Requirements”

ap. NPR 8621.1, “NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping”

aq. NPR 8705.2, “Human-Rating Requirements for Space Systems”

ar. NPR 8705.5, “Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects”

as. NPR 8715.3, “NASA General Safety Program Requirements”

at. NPR 8735.1, “Procedures for Exchanging Parts, Materials, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program and NASA Advisories”

au. NPR 8735.2, “Management of Government Quality Assurance Functions for NASA Contracts”

av. GLPD 8730.5, “NASA Glenn Quality Management System Policy”

aw. GLPR 1270.1, “Corrective and Preventive Action”

ax. GLPR 7123.35, “GRC Technical Review Procedure”

ay. GLPR 7150.1, “GRC Software Engineering Requirements”

az. GLPR 8040.1, “GRC Configuration Management & Data Management”

ba. GLPR 8700.4, “GRC Product Assurance”

bb. GLPR 8730.5, “Glenn Research Center Business Management System (BMS) Quality System Manual”

bc. GLPR 8730.6, “Control of Inspection, Measuring, and Test Equipment”

bd. GLM-QS-1700.1, “NASA Glenn Safety Manual”

be. GLM-QS-1800.1, “Occupational Health Programs Manual”

bf. GLM-QS-8500.1, “Environmental Programs Manual”

bg. GLM-QE-8730.1, “Parts Derating”

bh. GLHB-QE-8730.1, “EEE and Mechanical Parts Management Handbook”

Note 1: If a conflict exists between this document and any applicable NASA standards, the NASA standards ***shall*** *take precedent.*

Note 2: It is acknowledged that this document contains requirements that are applicable directly to engineering. This document has historically served as a placeholder for these requirements because engineering requirements documents did not exist. GRC engineering management has agreed that the engineering requirements and engineering best practices should be documented in engineering requirements documents and once these have been developed, those requirements will be removed from this document. Eventually, when all engineering requirements have been removed, this document will only contain safety and mission assurance requirements.

P.5 Reference Documents

a. ANSI/AIAA G-020-1992, “Guide for Estimating and Budgeting Weight and Power Contingencies for Spacecraft Systems”

b. MIL-HDBK-1811, “Mass Properties Control for Space Vehicles”

c. NASA-TM-86538, “Design and Verification Guidelines for Vibroacoustic and Transient Environments”

d. NASA-TM-106943, “Preloaded Joint Analysis Methodology for Space Flight Systems”

e. NASA TM X-73305, “Astronautic Structures Manual Volume I”

f. NASA TM 4322, “NASA Preferred Reliability Practices for Design and Test”

g. NASA-HDBK-5010, “Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware”

h. NASA-STD-8729.1, “Planning, Developing, and Managing an Effective Reliability and Maintainability Program”

i. S-313-100, “Goddard Space Flight Center Fastener Integrity Requirements”

j. CSG-RS-10A-CN, “Centre Spatial Guyanais Safety Regulation Volume 1”

k. CSG-RS-21A-CN, “Centre Spatial Guyanais Safety Regulation Volume 2–Part 1”

l. CSG-RS-22A-CN, “Centre Spatial Guyanais Safety Regulation Volume 2–Part 2”

m. CxP 70038, “Constellation Program Hazard Analyses Methodology”

n. ESA-ATV-PR-13830, “ATV Pressurized Payload/Cargo Safety Certification Process”

o. ESA-ATV-1700.7, “Safety Requirements for Payloads/Cargos On Board the ATV”

p. NASDA-ESPC-2857, “HTV Cargo Standard Interface Requirements Document”

q. NSTS/ISS 13830, “Payload Safety Review and Data Submittal Requirements for Payloads Using the Space Shuttle and International Space Station”

r. NSTS 1700.7, “Safety Policy and Requirements for Payloads Using the Space Transportation System”

s. NSTS 1700.7, “ISS Addendum: Safety Policy and Requirements for Payloads Using the International Space Station”

t. NSTS 16725, “Flight Test and Supplementary Objectives Document (FTSOD)”

u. P32928-103, “Requirements for International Partner Cargo Transported on Russian Progress and Soyuz Vehicles”

v. SSP 30309, “Safety Analysis and Risk Assessment Requirements Document (for the International Space Station)”

w. SSP 52005, “Payload Flight Equipment Requirements and Guidelines for Safety-Critical Structures”

x. SSP 50021, “Safety Requirements Document for International Space Station”

y. SSP 50448, “Station Development Test Objectives”

z. NPD 8720.1, “NASA Reliability and Maintainability (R&M) Program Policy”

aa. NPR 8705.6, “Safety and Mission Assurance Audits, Reviews, and Assessments”

ab. NPR 8715.3, “NASA General Safety Program Requirements”

ac. NPR 8715.7, “Expendable Launch Vehicle Payload Safety Program”

ad. GLPD 1150.3, “Fracture Control Working Group”

ae. GLPR 8000.1, “GRC Procedural Requirements for Risk Management”

af. GLPR 8700.4, “Product Assurance, GRC BMS Procedure”

ag. GLP-QE-3451.1, “Quality and Safety Achievement Recognition (QASAR) Award”

ah. GLP-QE-8700.3, “Space Product Assurance”

ai. GLP-QE-8700.4, “Lessons Learned Information System”

aj. GLP-QE-8700.1, “Roles, Responsibilities, and Interrelationships of SMAD/SSQRD Support to GRC Programs/Projects”

ak. GLP-QE-8730.2, “QA/QE Support to Projects”

al. GLP-QE-8730.3, “Customer Requested Audits and Surveys”

am. GLP-QE-8730.7, “Control of Inspection Stamp or Signature”

an. GLP-QE-8730.8, “Materials and Processes”

ao. GLP-QE-8735.1, “Government Industry Data Exchange Program (GIDEP) & NASA Advisories”

ap. GLM-QE-8700.1, “Product Assurance Manual”

aq. GLWI-QE-8730.9, “Materials and Processes Certification for Space Programs and Projects”

ar. GLWI-QE-8730.10, “Materials Usage Agreement (MUA)”

as. GLWI-QE-8730.6, “Design for Radiation”

at. SP-610S, “NASA Systems Engineering Handbook”

au. JSC 17481, “Safety Requirements Document for JSC Space Shuttle Flight Equipment”

av. JSC 23642, “JSC Fastener Integrity Testing Program”

aw. JSC 29353A, “Flammability Configuration Analysis for Spacecraft Applications”

ax. IPC-A-600, “Guidelines for Acceptability of Printed Boards”

ay. IPC-6011, “Generic Performance Specifications for Printed Boards”

az. IPC-6012, “Qualification and Performance Specification for Rigid Printed Boards”

ba. J-STD-004, “Requirements for Soldering Fluxes”

bb. J-STD-005, “Requirements for Soldering Pastes”

bc. J-STD-006, ”Requirements for Electronic Grade Solder Alloys and Fluxed and Nonfluxed Solid Solders for Electronic Soldering Applications”

P.6 Measurement/Verification

a. The GRC Program and Project Assurance Division (PPAD) conducts annual assessments of programs/projects to verify compliance with this document. Compliance will be determined by reviewing the archived artifacts required by this document.

b. Programs/projects should provide comments/feedback to the PPAD by use of the Corrective and Preventive Action Reporting System in accordance with GLPR1270.1 for future updates.

c. Independent Internal and External Audits of this procedure are also performed as part of the overall GRC Business Management System Quality System process per GLPR 8730.5.

P.7 Cancellation

a. None.

/S/
Ray Lugo
Deputy Director

Chapter 1. Responsibilities

1.1 GRC Management

a. Assigns program/project manager (PM) and program/project chief engineer (PCE) and program/project chief safety and mission assurance officer (CSO) to the program/project.

b. Ensures the technical integrity of the project through participation in reviews of program/project and technical plans.

c. Assists the program/project team with obtaining the institution capabilities necessary to plan and implement the program/project.

1.2 Project Manager (PM)

a. The PM is responsible for ensuring all safety and mission assurance requirements are satisfactorily accomplished.

b. The PM leads the development, approval, and maintenance of the project safety and mission assurance plan.

1.3 Project Chief Engineer (PCE)

a. Serves as the project-level engineering technical authority, and ensures that the project and technical planning is consistent with Agency and Center engineering design processes, specifications, rules, best practices, etc., necessary to fulfill this document's requirements for the project.

1.4 Lead Systems Engineer (LSE)

a. Leads all program/project systems engineering and integration (SE&I) activities. The LSE is responsible for the formulation and implementation of the assigned project SE&I element including the safety, technical integrity, performance, and mission success of the SE&I element while meeting (cost and schedule) commitments.

1.5 Chief Safety and Mission Assurance Officer (CSO)

a. Serves as the program/project-level safety and mission assurance (SMA) technical authority, and ensures that the program/project and technical planning is consistent with Agency and Center SMA design processes, specifications, rules, best practices, etc., necessary to fulfill mission performance requirements for the project.

b. The CSO ***shall*** assist the PM in ensuring the SMA requirements are satisfactorily accomplished and have direct access to project management.

c. Specifically, for program/project and technical planning, the CSO:

(1) Assures the development of the program/project SMA plan.

(2) Reviews and concurs on program/project and technical planning documents.

(3) Defines assigned element product breakdown structure, deliverables, facilities, and risks.

(4) Defines assigned element product specific schedule details, resource requirements and cost estimates, and requests Center-provided resources.

(5) Establishes use and maintains a system to report failures and nonconformances through a documented problem reporting and corrective action system.

d. Provides the SMA plan component to the Systems Engineering Management Plan.

1.6 System Safety Lead Engineer

a. The system safety lead engineer assures that the system safety requirements are placed in program/project requirements and that any variances to those requirements are processed in accordance with the requirements in this document.

b. Specifically, the System Safety lead:

(1) Assures the development of a system safety technical plan (SSTP) during the project formulation phase and update the plan throughout the system life cycle

(2) Ensures that system safety models are constructed to support the implementation of the risk-informed decision framework.

(3) Ensures that the system safety models incorporate all the safety attributes important to risk-informed decision making by working with the PM and other decision makers as deemed appropriate.

(4) Establishes the methods and tools that are used in the risk-informed framework.

(5) Checks and validates the methods and tools before implementation and obtain concurrence from the PM.

(6) Documents the basis for the methods and tools used and analytical results.

1.7 Reliability Lead Engineer

a. Reliability lead engineer assures that the reliability, maintainability, and probabilistic risk assessment requirements are placed in program/project requirements and that any variances to those requirements are processed in accordance with the requirements in this document.

b. Specifically, the reliability lead:

(1) Ensures that reliability and maintainability (R&M) activities (addressing hardware, software, firmware, human elements, and interactions between them) are planned and implemented.

(2) Ensures that R&M data is available for use as heritage data to support the formulation of R&M goals and requirements, quantitative and qualitative reliability analysis, and other R&M engineering activities as part of current, follow-on, or new programs and projects.

(3) Ensures programs/projects conduct and use probabilistic risk assessment with the best state-of-practice methods and data to support management decisions to improve safety and performance.

1.8 Materials and Processes (M&P) Lead Engineer

a. The M&P lead engineer assures that the M&P requirements are placed in program/project requirements and that any variances to those requirements are processed in accordance with the requirements in this document.

b. Specifically, the M&P lead:

(1) Ensures that the project is in compliance with their materials selection, control and implementation. The M&P lead engineer will offer solutions to projects on M&P issues and network with subject matter experts, as needed, to assist the project.

(2) Provides assistance to the program/project in planning and implementing any material testing of hardware required.

(3) Assists and advises the program/project on the material certification process.

(4) Drafts the certification letter and forwards it to the Safety and Mission Assurance Directorate certification official.

1.9 Quality Assurance (QA) Lead Engineer

a. The QA lead engineer assures that the QA requirements are placed in program/project requirements and that any variances to those requirements are processed in accordance with the requirements in this document.

b. Specifically, the QA lead:

(1) Ensures program planning and acquisition documents incorporate applicable requirements of this document, including specification of applicable quality system requirements.

(2) Ensures applicable QA requirements down to successive levels of the supply chain to ensure control of subtier suppliers and verification of safety/mission critical attributes at all levels of the supply chain.

(3) Identifies safety/mission critical attributes and associated government mandatory inspection points.

(4) Ensures the collection and analysis of quality data for the purpose of identifying and initiating resolution of problem areas, common deficiency causes, nonconformance trends, defect anomalies, and process variations.

1.10 Software Assurance SA Lead Engineer

a. The SA lead engineer assures that the software safety, reliability, and assurance requirements are placed in program/project requirements and that any variances to those requirements are processed in accordance with the requirements in this document.

b. The SA lead engineer works with a program/project to review, analyze, advise, and report on the software development process. In addition, they report all mission-critical and safety-critical findings to the Office of Safety and Mission Assurance, as well as program, and/or project management.

Chapter 2. Overall Responsibilities

2.1 Description of Overall Requirements

a. The GRC program/project manager (PM) has primary responsibility for ensuring assurance requirements are satisfactorily accomplished. However, the Chief Safety and Mission Assurance Officer (CSO) ***shall*** assist the PM in this effort and has direct access to developer management. The safety and mission assurance (SMA) program ***shall*** operate concurrently with all other elements.

b. The project is required to plan, implement, and organize a SMA program that encompasses all flight hardware, software, government-furnished equipment, and support equipment from initiation through development and subsequent missions or tests (see Section 2.2). The SMA program ***shall*** be in place throughout the life cycle of the program or project, whether the hardware is placed in storage or until the associated hardware and software are retired.

c. The SMA program applies to all work accomplished by the project including contractors, subcontractors, and suppliers. The development may be in-house or by an outside contractor.

2.2 Safety and Mission Assurance Plan

a. The SMA support, dictated by the CSO, ***shall*** be implemented with an approved Safety and Mission Assurance Plan (SMAP), which addresses all sections of this space assurance requirements (SAR) directive. The SMAP ***shall*** document how the program/project is going to meet the requirements within this directive. The SMAP ***shall*** also include SAR reference paragraphs, deliverables, and performing organizations. Any noncompliance to the requirements in the SAR ***shall*** be identified and justified in the SMAP. Verification to SAR requirements ***shall*** be satisfied by successful completion of the program and project reviews, verification as defined in the SMAP and release of the associated data products listed in the contract. Appendix C provides a cross-reference matrix to the SAR requirements and the program/project verification method. The SMAP ***shall*** be reviewed and approved by the PM and CSO. Any proposed changes to the approved SMAP ***shall*** be submitted to the PM and CSO for approval prior to implementation. Projects are encouraged to make maximum use of their own existing procedures. Procedures referenced in an approved SMAP ***shall*** also be available for information at the developer's facility.

b. For an outside contract, the SMAP ***shall*** be delivered by the effective date of the contract in accordance with the contract schedule. The contractor's practices and procedures referenced in the SMAP ***shall*** also be delivered at the effective date of contract in accordance with the contract schedule. If any inconsistencies between the approved SMAP and the SAR become evident during the contract period of performance, the SAR ***shall*** take precedence, except when specific noncompliances have been approved by the PM and CSO. Any new procedure or any proposed changes to the approved procedures ***shall*** be submitted to the PM and CSO for review and/or approval in accordance with the contract.

c. Table 2-1 lists all of the different control plans that are described throughout this document, and will be required to be considered for development.

Table 2-1—Control Plans

Description	Paragraph
Safety and Mission Assurance Plan	2.2
Storage Plan	2.3.1
Mishap Preparedness and Contingency Plan	2.7
Verification Plan	3.2
Fracture Control Plan	3.4.5
Systems Safety Technical Plan	4.4
EEE Parts Control Plan	5.2.1
Mechanical Parts Control Plan	5.3.1
Materials and Processes Selection, Control, and Implementation Plan	6.1
Reliability, Availability, Maintainability Plan	7.1.4
Probabilistic Risk Assessment Plan	7.2.7
Quality Assurance Plan	8.1
Configuration Management Plan	8.3
Contamination Control Plan	8.7.1
Risk Management Plan	9.3
Software Assurance Plan	10.1
Software Configuration Management Plan	10.4

2.2.1 Use of Deviations

a. A deviation ***shall*** be written for each SAR requirement that the program/project does not meet. The deviation ***shall*** be submitted to the PM and the CSO for review. Each deviation ***shall*** be stored in an appendix in the SMAP. The process defined in *GLPR 7120.14 (under development)*, "GRC Deviation/Waiver Process," ***shall*** be used to document and approve agreements affecting specific requirements that intentionally release a project from meeting that requirement.

2.3 Use of Previously Designed, Fabricated, or Flown Systems

a. When a system that was designed, fabricated, or flown previously is to be used, the developer is required to demonstrate how the system complies with the SMA requirements in this document. Furthermore, to avoid repeating certain tasks, which previously demonstrated the system complied with requirements, the developer ***shall*** have evidence from the previous program or project that shows how flight worthiness and the integrity of the system were maintained. At a minimum, a verification readiness review (VRR) ***shall*** be conducted for any reflights to address the reverification and test program.

b. Programs and projects should have plans in place to disposition the hardware at mission completion.

2.3.1 Storage Requirements for Suspended Projects

a. Suspended projects and projects subject to a prestorage review ***shall*** assure that the hardware, software, and documentation that they have developed are appropriately stored and maintained for future use.

b. The PMs of suspended (or prestorage review) projects with qualification (prototype), protoflight, or flight hardware/software ***shall*** prepare a storage plan to define specific storage constraints and activities to be conducted before, during, and after storage. The storage plan must include, but is not limited to:

(1) A detailed list of the hardware, software, and documents being stored

(2) The status of the flight system going into storage, including completed verification activities, outstanding problem reports, and waivers/deviations

(3) The configuration for storage, including the appropriate drawings and procedures to be followed to go from flight configuration to storage configuration and back

(4) Expected/acceptable length of the storage period, including any operational or maintenance requirements and plans (e.g., replacement of limited-life items and periodic inspection and/or testing)

(5) Operational limits during storage (to ensure sufficient life remains for the mission)

(6) Handling and storage requirements, including safety precautions, temperature, and humidity

(7) Attributes of the storage area(s), including environmental controls, accessibility controls (i.e., bonded storage), and requirements for periodic QA monitoring

(8) Plans for temporary archiving of project data and records (if needed) and for maintaining configuration control of all items stored

(9) Post storage plans, including replacement of limited-life items (e.g., batteries) and verification activities (e.g., testing) to demonstrate integrity and flight readiness of the stored item(s)

(10) Identification of project risks and mitigation strategies once the hardware comes out of storage

(11) The version of flight and GSE software (executables and source code) and how stored

(12) Identification of the software configuration management system and how this system is implemented (local server, Web based, etc.)

(13) Identification and use of software development tools that are required to run the flight and/or ground software (e.g., compilers)

c. All project records must be maintained per NPR 1441.1.

d. The storage area environment and accessibility must be controlled, as needed, to prevent damage, deterioration, or loss of the items stored. The storage area must be checked periodically to verify controls are functioning properly and stored items continue to be well maintained.

2.4 Assurance Status Reports

a. The program/project ***shall*** submit SMA Status Reports on a quarterly basis to the PM and CSO. The reports ***shall*** cover items such as those listed below as well as those discussed in the individual sections of this document:

(1) Key SMA organization and personnel changes

(2) Significant SMA risks

(3) Safety and deviation/waiver issues

(4) Status of SMA activities in manufacturing, testing, and operations

(5) Supplier and subcontract SMA activities

(6) Audit, nonconformance, and problem reports

(7) Review status

(8) Parts list, parts problems, and ALERT findings

(9) Performance and problem trend analyses

2.5 Contractor Surveillance

a. The GRC ***shall*** use a surveillance approach to evaluate the contractor and determine if contract performance is acceptable. The government's objective is to balance the level of surveillance with the perceived impacts and risks of meeting program/project goals. The GRC programs/projects ***shall*** identify program requirements, strategy, resources, review and control processes, surveillance activities, and metrics for continuous measurement of the contractor's performance.

b. The work activities, operations, and documentation performed on the program/project by a contractor, subcontractor, or supplier are subject to evaluation, review, audit and/or inspection by the government or its designated representatives as specified in the contract. When necessary, GRC will delegate responsibilities and authority to other government agencies in a letter of delegation or with an independent assurance contractor with a GRC contract, as appropriate.

c. The contractor, upon request, ***shall*** provide SMA documents, records, and equipment required to perform these activities to government representatives. The contractor ***shall*** also provide the government representatives with an acceptable work area within its facilities when requested.

2.6 GRC Assurance Review Requirements

a. The project ***shall*** support a series of formal or informal comprehensive system and subsystem-level design reviews per GLPR 7123.35, "GRC Technical Review Procedures." The reviews cover all aspects of project hardware, software, and operations for which the project has responsibility.

2.7 Mishap Reporting and Investigation

a. The project ***shall*** develop a Mishap Preparedness and Contingency Plan consistent with the requirements of NPR 8621.1B, and *GLPR 1720.1 (under development).* The project ***shall*** use the Incident Reporting Information System (IRIS) for documenting any reportable mishaps. The initial notification will be made within 24 hours of the mishap.

2.8 Safety, Health, and Environmental

a. The Glenn Safety and Health Management System (GSHMS) and Environmental Management System apply to all activities, operations, and organizations at GRC, both Lewis Field and Plum Brook Station. It is policy to manage and conduct research and development operations in such a manner as to eliminate or minimize all potential hazards and to avoid accidents involving injury to personnel, damage to property, negative environmental impact, or loss of research operating time and effectiveness as referenced in the NASA Glenn Research Center Safety

Manual (GLM-QS-1700.1), the Occupational Health Programs Manual (GLM-QS-1800.1) and the Environmental Programs Manual (GLM-QS-8500.1).

Chapter 3. Design and Verification

3.1 General Requirements

a. The program/project ***shall*** develop a verification approach that meets the requirements of *GLPR 7123.11 (under development)*, “Stakeholders Expectations, Requirements, Development, and Management.” The process for finalizing the verification plan, development of verification procedures, and the conducting of verification activities ***shall*** be per *GLPR 7123.22 (under development)*, “GRC Verification and Validation Procedure.”

b. The programs/projects ***shall*** complete a verification plan to ensure that all verification requirements (program/science, safety, assurance, interface, and operational) for the program/project are satisfied. The program/project plan contains the requirement sources and hierarchy and should include scope, tasks, methods, tools, metrics, risks, and resources as applicable to fulfill the purpose of the plan. The program/project plan ***shall*** be developed per *GLPR 7123.31(under development)*, “GRC Project and Technical Planning.” It is not further described in this document. Program/project assurance requirements that ***shall*** be verified are defined in this section and throughout the rest of this document. The overall verification program approach for project requirements are described generally in this section.

c. The program/project assurance requirements that are described in this section address integration and functional testing in the following areas: electrical, structural, electromagnetic interference (EMI), thermal and end-to-end systems test. The program/project will determine which integration requirements documents need to be followed. These documents provide the basis for the integration testing that is required in these areas. The functional testing requirements are based on GRC experience and practices developed over the years on a variety of programs.

d. Payload integration with the experiment carrier (e.g., Get Away Special (GAS)-can, hitchhiker) as described in this section is worked directly with the integration centers. Integration of the payload/carrier with the shuttle or other launch vehicle is the responsibility of the integration center with support from the payload developer. Payload test requirements ***shall*** meet NASA-STD-7002.

3.2 Overall Verification Program

a. A verification program begins with the development of a verification plan that identifies the program/project verification requirements, defines the method(s) of verification, provides traceability to original requirements, defines the requirement applicability to systems, and describes compliance. It concludes when the required verifications are completed (compliant or approved nonconformance) as outlined in the plan.

b. The methods of verification include analytical investigations, physical property measurements, inspections, and tests that include simulating the environments to be encountered. These environments may include handling and transportation, prelaunch, launch, onorbit, retrieval, reentry, and landing. For the assurance requirements found in this document, the prescribed method is defined along with the requirement.

c. The verification plan ***shall*** be initiated following the systems definition review and ***shall*** be consistent with *GLPR 7123.11(under development), GLPR 7123.22 (under development), and GLPR 7123.31(under development)*. The implementation can be at the component, subsystem, or system levels of assembly, which should be outlined in the verification plan.

d. Prior to preliminary design review (PDR), a coordination meeting should be held that includes GRC payload integration testing experts in the following test areas: electrical, structural, EMI, thermal, and systems. The purpose of the meeting ***shall*** be to identify the experiment unique characteristics that will drive the design and verification in these areas, and make the program/project team and the PM aware of the risks so that mitigation can be tracked in a timely and effective manner as detailed in Chapter 9.

e. All flight operations or other program/project activities ***shall*** undergo acceptance testing in accordance with the flight, reflight, or other program/project verification plan. All prototype or protoflight systems ***shall*** undergo qualification to demonstrate compliance with the requirements outlined in the verification plan. When hardware is selected for reflight, a prototype approach is preferred in order to clearly demonstrate design life margins. Additional requirements and guidance for test specifications and reporting is in Chapter 8, Quality Assurance.

f. The verification plan ***shall*** contain a verification matrix, which contains the following information:

(1) Requirements Document-identify the source document from which the verification element was obtained.

(2) Paragraph Reference-identify the paragraph from the source document.

(3) Requirement Title-specify the specific requirement in a brief descriptive form.

(4) Methods of Verification-identify methods of verification.

(5) Verification/Validation Approach Summary-verify the integrity, space worthiness, and capability of the flight system to perform the mission requirements.

(6) Closure Requirement-specify how closure will be accomplished and documented.

(7) Safety Closure Reference-identify any safety closure documentation.

(a) The verification matrix, as well as the verification plan, must be updated throughout the program/project to reflect the latest documentation and status changes. Updates of the matrix ***shall*** be provided to the GRC Project Office and to the GRC Safety and Mission Assurance Directorate.

3.3 Electrical Verification Requirements

a. The program/project ***shall*** demonstrate compliance with the electrical requirements as defined in the verification matrix by inspection, demonstration, similarity, analyses, or tests. Before the integration of an assembly, component, or subsystem into the next higher level system assembly, electrical interface, and bonding tests ***shall*** be performed to verify that all bonds, software, and signals are within acceptable limits of applicable performance specifications. Bonding ***shall*** be per NASA-STD-4003, “Electrical Bonding for NASA Launch Vehicles, Spacecraft, Payloads, and Flight Equipment.” For flight subsystems, all sections of the system's outer shell ***shall*** be bonded together to permit large quantities of electric charge to distribute across the shell by conducting paths and ***shall*** meet the requirements of NASA-STD-4005, “Low Earth Orbit

Spacecraft Charging Design Standard." NASA has established lightning protection requirements for design.

b. Solar cells and solar panels ***shall*** meet the requirements of American Institute of Aeronautics and Astronautics (AIAA) S-111-205, "Qualification and Quality Requirements for Space Solar Cells," and AIAA S-112-205, "Qualification and Quality Requirements for Space Solar Panels."

c. Additional inspection and test requirements are defined in Section 8.

3.4 Structural and Mechanical Requirements

a. The developer ***shall*** demonstrate compliance of the flight hardware with all structural and mechanical requirements for flight and ground safety and mission assurance, including those for mechanical interfaces and mass properties. The program/project must also demonstrate compliance with the structural and mechanical requirements for ground support equipment (GSE).

b. The verification plan that the program/project will write ***shall*** include a structural verification plan and mass properties control plan, and for Shuttle and International Space Station (ISS) payloads it must include a fracture control plan and a fastener integrity plan. The verification plan ***shall*** list the structural and mechanical requirements and their origin. It ***shall*** also state the method of verification (analysis, test, or inspection) for all appropriate ground and flight environments. These environments may include thermal and structural loads, vibroacoustics, mechanical shock, and pressure profiles that occur during ground handling and transportation, launch and landing, onorbit operation, and crew handling.

3.4.1 Safety- and Fracture-Critical Structures

a. The structural integrity of the flight hardware is a critical flight safety concern. Thus, extensive verification is required for safety-critical structures (SCS). The primary load path is defined as the collection of structural elements, which transfer load from one part of a structure to another. All structural elements including associated interfaces, fasteners, and welds in the primary load path, pressure systems, uncontained glass, rotating machinery, mechanical stops, and containment devices, are considered safety critical and ***shall*** be analyzed. Structural elements associated ***shall*** have positive margins of safety. Structural test against penetration ***shall*** be verified for containment devices.

b. The SCS may include a subset of components whose failure would present catastrophic hazards, that is, they are not fail-safe. These components are termed "fracture critical" and ***shall*** be shown through analysis, inspection, and/or test to be safe from failure throughout the mission. In practice, any damage to Space Transportation System (STS) or ISS hardware is considered catastrophic even though the crew and vehicle may not seem to be in danger. For manned space flight systems and payloads, the hardware developer will be required to develop and implement a fracture control plan, which incorporates life prediction, quality control and traceability, and in-depth inspection for those components classified as fracture critical.

c. The program/project should obtain a users handbook that defines the interfaces and environments for which the payload must be designed, and the carrier-specific structural verification requirements.

d. While the concepts of safety- and fracture-critical structures are intended to address mission safety, the hardware developer must also address the functional integrity of the hardware

(Mission Assurance). The carrier's concern is that the payload is safe. The program/project's concern is that the hardware works. Such "functional-critical" structures may include optical bedplates, lens brackets, actuators, and mechanisms, which are not safety-related but must survive predicted environments to meet functional requirements.

3.4.2 Structural Loads

a. NASA-STD-5002 ***shall*** be utilized for defining methodologies, practices, and requirements for conducting load analyses for payloads and spacecraft. Individual carrier/vehicle requirements should also be considered as well.

b. Flight hardware ***shall*** be designed to maintain structural integrity and functionality during all phases of the expected life cycle. Verification of the hardware to the structural load environments requires a combination of test and analysis. Flight structures and systems ***shall*** consider static and dynamic loads encountered during assembly, testing, transportation, launch, ascent, space operations, extraterrestrial operations, descent, and landing. Hardware is generally exposed to the following three types of flight environments during its launch and ascent loading events: (1) low-frequency (0- to 50-Hz) dynamic transient excitation, (2) high-frequency (20- to 2000-Hz) random vibration excitation, and (3) high-frequency (31 to 10 000 Hz) acoustic excitation.

c. Estimation of loads for the payload is an iterative process throughout the life cycle of the hardware until launch. Preliminary design loads are used for the initial sizing of the structure. Next, a mathematical model of the structure is developed and a preliminary load cycle is performed. Subsequent load cycle analyses are needed to assess the changes in design, and in the launch vehicle and payload mathematical models, and in forcing functions. Typically, a minimum of two load cycles are performed: a preliminary load cycle, which uses models based on initial sizing, and a verification load cycle that uses test-verified models. Uncertainty factors should be used in early load cycles to reduce design impacts associated with immaturity in models and design. Verification of the payload model by modal survey testing ***shall*** be performed to ensure the model is sufficiently accurate for load and deflection predictions.

d. Limit load is the maximum anticipated load experienced by a structure during a loading event. For cases where loads produced by different sources occur simultaneously, these loads ***shall*** be combined according to established techniques to define the limit load for that flight event. One common example of load combination occurs during launch, which exposes the payload to both low-frequency dynamic transient loads and to high-frequency random vibration loads. A typical approach used to combine loads in a case like this is to root-sum-square (RSS) the maximum low- and high-frequency loads.

3.4.3 Factors of Safety

a. Factors of safety (safety factors) are multiplying factors to be applied to limit loads or stresses for purposes of analytical assessment (design factors) or test verification (test factors) of design adequacy in strength or stability. NASA-STD-5001 establishes design and test factors, as well as service life factors, to be used for space flight hardware development and verification.

3.4.4 Margins of Safety

a. All structural elements critical for safety and mission assurance ***shall*** be shown by analysis to have positive margins of safety or, in the case of containment devices, be structurally adequate against penetration. The Margin of Safety (MS) is defined as

$$MS = \frac{Allowable\ Load}{FS \times Limit\ Load} - 1$$

b. where the Factor of Safety (FS) is for the load.

c. The minimum MS for all credible failure modes must be determined. A list would include such things as tensile failure, yielding, shear tear-out, excessive deflection, crippling, and joint separation. An excellent resource for determining the allowable load for various structural members is NASA TM X–73305.

d. NASA–TM–106943 is a detailed guide for performing bolted joint analysis.

e. The determination of MS for a payload is normally a labor-intensive process. Typically, a math model (Finite Element Model) is generated. This model is exercised for all load cases, and the resulting member loads are determined. These member loads are used in hand calculations to MS for the credible failure modes. The analyses must be well documented in a stress report, and must be updated for the as-built condition or any redesign of the hardware. The math model must normally be verified with a static test unless a “no test” approach has been approved.

f. Formal checking of all calculations, by a third party, is an industry-standard practice and is recommended for all space flight hardware. Checking can add 30 percent to the cost of an analysis but can uncover potentially deadly or costly errors. One hundred percent checking ***shall*** be mandatory for the “no test” approach.

g. Formal checking and review should not be confused. In formal checking, all hand calculation sheets are checked line by line for method used, assumptions, inputs, and accuracy of results. Programmed calculations (e.g., Excel spreadsheets, Matlab models, etc.) are subject to the same criteria and must be verified for accuracy of results. The use of industry standard software analysis programs should be checked for appropriate selection of program, features, and options consistent with the design approach. Finite Element Analysis solutions, for example, should be checked for modeling techniques, boundary conditions, material property selection, units, applied loads and other inputs, as well as for proper interpretation of the output. A number of global checks can be performed including mass properties, equilibrium, rigid body modes, etc., and the third-party checker can verify that these were properly done. Hand-calculations of MS that utilize Finite Element Analysis outputs such as member and joint loads must also be verified. Typically, an experienced engineer, from the same discipline and one who understands the methodologies, will perform the formal checking and sign off each sheet after reconciling any differences with the originator. Checking is a “quality control” task of the performing organization, not a government insight/oversight task.

h. Reviewing, on the other hand, is done at a higher level and lower fidelity than checking. A reviewer will page through the analysis report to see if everything is covered and seems to make sense, and perhaps do a few spot checks. The reviewer may even go deeper in a few areas that are deemed critical. However, this will not catch most errors that a third-party checker would catch. The reviewer usually signs and dates a signature page but nothing else. Review is the responsibility of the performing organization but also may be a government insight/oversight task.

3.4.5 Fracture Control

a. All manned space flight systems ***shall*** be subjected to fracture control to preclude catastrophic failure. The NASA-STD-5019 establishes requirements for fracture control of all NASA manned space flight hardware. The NASA-STD-5003 provides supplementary requirements specifically for payloads using the space shuttle. The NASA-HDBK-5010 provides guidelines and examples as a supplementary document to the NASA-STD-5019 and NASA-STD-5003 for fracture control implementation.

b. The fracture control process consists of the following elements, which are described in further detail in NASA-STD-5019:

(1) Responsible Fracture Control Board (RFCB). The RFCB is the designated board at the NASA Center or sponsoring institution responsible for the fracture control methodology. It is responsible for approving the program/project's hardware specific fracture control plan and fracture control summary report and for assuring compliance with the requirements of NASA-STD-5019 and carrier-specific documents.

(2) Fracture Control Plan. The program/project ***shall*** develop a fracture control plan that provides detailed hardware-specific fracture control methodology and procedures for the prevention of catastrophic failures associated with the propagation of cracks. The payload-specific fracture control plan must be approved by the fracture control authority.

(3) Fracture Classification. All space flight hardware parts must be examined to determine their fracture criticality classification. A part is designated fracture critical if it is credible that cracks in the part could lead to a catastrophic failure. For composite materials, the term crack also includes delaminating, defects due to manufacturing, impact damage, and in-service damage.

(4) Damage Tolerant Analysis or Test. The life of all fracture-critical parts must be assessed using damage tolerant fracture mechanics analyses. Damage tolerant testing can be used whenever damage tolerant analysis methodologies are not applicable or in lieu of analysis if approved by the RFCB. The parts must be shown to resist failure due to the presence of cracks during the entire service life multiplied by the required service-life factor. The service-life factor for all NASA space flight hardware on manned systems ***shall*** be four.

(5) Traceability. Traceability of materials, design changes and analyses, manufacturing processes, inspections, environmental exposure, and load history ***shall*** be maintained on all fracture-critical parts throughout the hardware development, manufacturing, testing, and flight phases.

(6) Nondestructive Evaluation (NDE). All fracture-critical parts must be subjected to NDE or proof testing to screen for internal and external cracks.

(7) Fracture Control Summary Report. To certify fracture control compliance, the hardware developer must provide a fracture control summary report on the entire flight system for review and approval by the fracture control authority. The report ***shall*** include an accounting of all parts and the basis for determining their acceptability.

c. The requirements of NASA-STD-5019 are not imposed on systems other than manned space flight but may be tailored for use in specific cases where it is prudent to do so, such as when national assets are at risk.

3.4.6 Pressurized Systems

a. Pressurized systems on space flight vehicles and payloads are of special concern because of the potential for sudden, catastrophic energy release, the release of hazardous fluids, the unusual environments encountered in space flight, and the low MS often required to obtain acceptable system weight. For human space flight, pressurized systems are covered by the requirements of fracture control (see Section 3.4.5). Pressurized systems for manned space flight must be two-failure tolerant regarding pressure; that is, the Maximum Design Pressure (MDP) must not be exceeded with any combination of two credible failures.

b. Pressurized systems to be flown on unmanned vehicles ***shall*** meet the requirements of ANSI/AIAA S-080, Space Systems-Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, and ANSI/AIAA S-081, Space Systems-Composite Overwrapped Pressure Vessels (COPV).

3.4.7 Strength Testing

a. Structural designs of space flight systems must generally be verified by both analysis and by either prototype or protoflight strength testing. The standard accepted practice for verification of launch vehicles is the prototype approach in which a separate, dedicated test structure, identical to the flight structure, is tested to demonstrate that the design meets the factor of safety requirements.

b. A widely used acceptable alternative for verification of spacecraft and science payloads is the protoflight approach, wherein the flight structure is tested to levels somewhat above limit stress (or load) but below yield strength. Test Factors of Safety for both protoflight and prototype approaches are identified in NASA-STD-5001.

c. Strength verification tests fall into three basic categories: tests to verify strength of the design (qualification, acceptance, or proof), tests to verify strength models (the finite element models used in calculating MS), and tests to verify workmanship and material quality of flight articles (acceptance or proof).

d. Strength verification tests are normally static load tests covering all critical load conditions in the three orthogonal axes. Acceleration loads are simulated by strategically placed linear actuators. The magnitude of the static test loads should be equivalent to limit loads multiplied by the qualification, acceptance, or proof test factor. In some cases, alternative test approaches (centrifuge, below resonance sine burst, saw tooth shock, etc.) may be used in lieu of static testing if it can be demonstrated that the resulting loads in the test article are equivalent to or larger than the limit loads multiplied by the test factor. However, the ability to perform these alternative tests is usually limited by the mass and size of the test article.

e. Strength model verification tests are normally done as part of the strength verification tests. Model verification must be accomplished over the entire load range. The test article must be adequately instrumented to provide sufficient test data for correlation with the strength model.

f. Under some circumstances, it may be permissible to verify structural integrity by analysis alone without strength testing, provided an acceptable engineering rationale is developed.

g. Standard criteria cannot be specified for general use in designing structures for which no verification tests are planned. Programs/projects, which propose to use the “no-test” approach generally, must use larger factors of safety and develop project-specific criteria and rationale for

review and approval by the GRC Engineering Review Board and by the payload carrier. For spacecraft and other payloads launched on the space shuttle, these criteria must be approved by the Space Shuttle Payload Safety Review Panel prior to their implementation.

3.4.8 Vibroacoustics

a. The purposes of vibroacoustic (acoustic and random vibration) testing, with test factors, are: (1) to prove design performance at the maximum expected flight level (MEFL), plus margin for uncertainty, (2) to demonstrate that hardware is acceptable for flight, and (3) to verify that adequate workmanship exists in the construction of the hardware.

b. To satisfy the vibroacoustic requirements, a space flight hardware test verification plan ***shall*** be developed which is based on an assessment of the expected mission environments and the type of flight hardware program (prototype or protoflight). NASA-STD-7001 states very clearly the requirements for space flight hardware, and these requirements ***shall*** be enveloped with the carrier mission requirements. An executive summary of NASA-STD-7001 is given in Table 3.4-1.

Table 3.4-1—Executive Summary of NASA-STD-7001 Verification Test Requirements[3]

Type of Test Hardware	Test Level[1,2]	Test Duration
Prototype:		
Qualification:		
Single Mission	MEFL + 3 dB	2 minutes per axis
Multiple (N) Reflights:	MEFL + 3 dB	2 + 0.5N minutes per axis N = Number of reflights
Flight Acceptance:	MEFL - 3 dB	1 minute per axis
Protoflight:	MEFL + 3 dB	1 minute per axis

[1]Notes: Maximum Expected Flight Level (MEFL) defined as 95 percent/50 percent probability level.
[2]A minimum workmanship random vibration test specification (of 6.8 grms) ***shall*** be imposed on electrical, electronic, and electromechanical components weighing 50 kg (110 lb) or less. This spectrum is given in Table 3.4-2.
[3]Check the parent document for current test levels.

3.4.8.1 Component Random Vibration Testing

a. Random vibration testing is required for essentially all electrical, electronic, and electromechanical components and mechanisms. Exceptions include large area-to-weight structures (which may be subjected to acoustic testing) and hardware not practical to vibrate at the component level (which may be more easily tested at the subsystem level, such as cabling, plumbing, and blankets).

b. Random vibration tests, in three axes, ***shall*** be performed at the component level of assembly to the test levels and durations specified in NASA-STD-7001. If appropriate, as specified in Section 3.4.8.1.1, these test levels ***shall*** also envelope the component minimum workmanship levels.

3.4.8.1.1 Workmanship

a. Workmanship random vibration testing is performed to identify latent defects and manufacturing flaws in electrical, electronic, electromechanical, and mechanism hardware at the component level. The minimum workmanship level provided in NASA-STD-7001 is shown in Table 3.4-2 and has been proven an appropriate level for workmanship screening. Thermal stress

screening is also highly recommended, but it does not replace the workmanship random vibration screening.

Table 3.4-2—Component Minimum Workmanship Random Vibration Test Levels

Frequency	Test Level
20 Hz	0.01 g^2/Hz
20 to 80 Hz	+3 dB/octave
80 to 500 Hz	0.04 g^2/Hz
500 to 2000 Hz	–3 dB/octave
2000 Hz	0.01 g^2/Hz
Overall Level	6.8 G_{rms}

b. The minimum workmanship random vibration test specification ***shall*** be imposed on electrical, electronic, and electromechanical components weighing 50 kg (110 lb) or less. It need not be applied to components weighing greater than 50 kg (110 lb).

c. When the minimum workmanship test level exceeds the qualification/flight acceptance/ protoflight levels, the random vibration test level ***shall*** envelope the two spectra. Thus, the workmanship level may often drive the test level for hardware flying in relatively benign flight environments, such as a space experiment being launched in the shuttle.

d. Care should be exercised not to apply workmanship to highly vibration-sensitive optical components and sensors that could be damaged by these levels. Examples of possible exceptions might include mirror assemblies, alignment critical devices, and optical hard drives. For these exceptions, some confidence of sufficient workmanship should be obtained by other means such as by inspection or vendor data.

3.4.8.1.2 Stowed Components

a. Hardware designed and launched in a stowed condition ***shall*** satisfy the following two conditions:

(1) A qualification/protoflight test in the stowed configuration ***shall*** be performed. This test is to verify that the packaging requirements are sufficient and/or that the flight package design itself can survive the launch environments with margin.

(2) Electrical, electronic, and electromechanical components weighing 50 kg (110 lb) or less ***shall*** be exposed to workmanship levels via either testing in the stowed or hard-mounted configuration. This test is to verify adequate workmanship of the flight/protoflight hardware and identify latent defects that could cause on-orbit failure (despite package protection during launch), particularly in light of loads and stresses imposed by handling and transportation. Highly vibration-sensitive flight/protoflight hardware will only be screened to the vibration levels seen in the stowed configuration test (which is likely to be below the 6.8 G_{rms} workmanship level).

b. The recommended logic to determine what testing should be performed is provided in Figure 3.4-1 and Figure 3.4-2, for protoflight and prototype projects, respectively. For the evaluation of new flight packaging concepts, it may be beneficial to test first with a mass simulator unit, before testing with the actual hardware.

c. A hard-mounted workmanship test of the flight/protoflight hardware is likely to be required. When utilizing efficient flight packaging design, this test may actually drive the hardware design. In these cases, it may be appropriate to first perform a qualification test of the hardware in its hard-mounted configuration to relieve concern.

3.4.8.1.3 Retesting of Reflight Hardware

a. The NASA-STD-7001 states that test tailoring may be allowed, if technically justified, for the retesting of reflight hardware. The incorporation of a prototype flight hardware program is highly recommended if it is expected that flight hardware will be utilized for multiple missions. The qualification testing performed in a prototype program will greatly aid in assessing the remaining life in the flight hardware. The amount of testing and reverification needed to assess the reflight hardware is unique in each case. This assessment should be based on the design changes (if any) to the hardware, the amount of reassembly and refurbishment required, and on whether the dynamics of the structure have been changed (e.g., different structural interfaces and different carrier).

3.4.8.2 Additional Vibroacoustic Testing

a. Vibroacoustic testing ***shall*** be performed at the subsystem level, if appropriate, per NASA-STD-7001. Workmanship is not to be applied at the subsystem level of assembly. Subsystems undergoing random vibration testing may have their test levels reduced in order to prevent an over test at the resonance of the vibration test fixture.

b. An acoustic test may be required for large area-to-weight ratio structures (such as skin panels, reflectors, dish antennae, and solar panels) that respond significantly to the direct impingement of the acoustic environment.

c. Additional vibroacoustic tests ***shall*** be included in the test program if appropriate. For example, sine vibration may be added to simulate sustained oscillations occurring during the launch, or as an alternative method of satisfying another requirement such as loads testing.

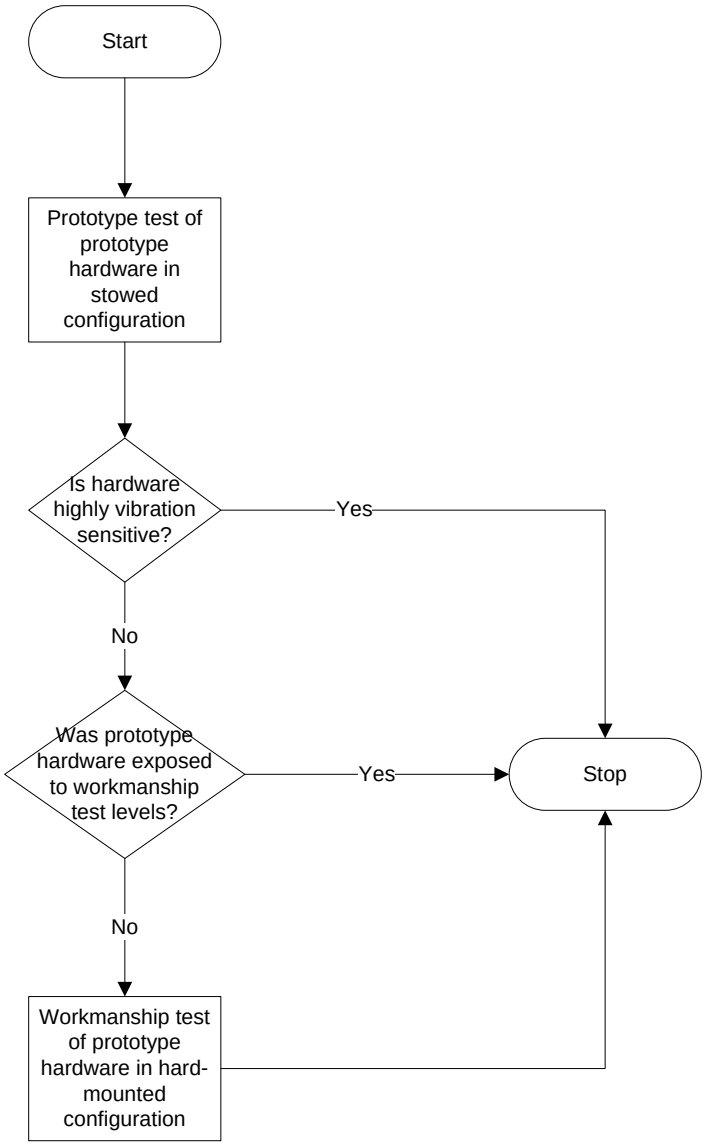

Figure 3.4-1—Vibration Testing of Stowed Hardware for Protoflight Project.

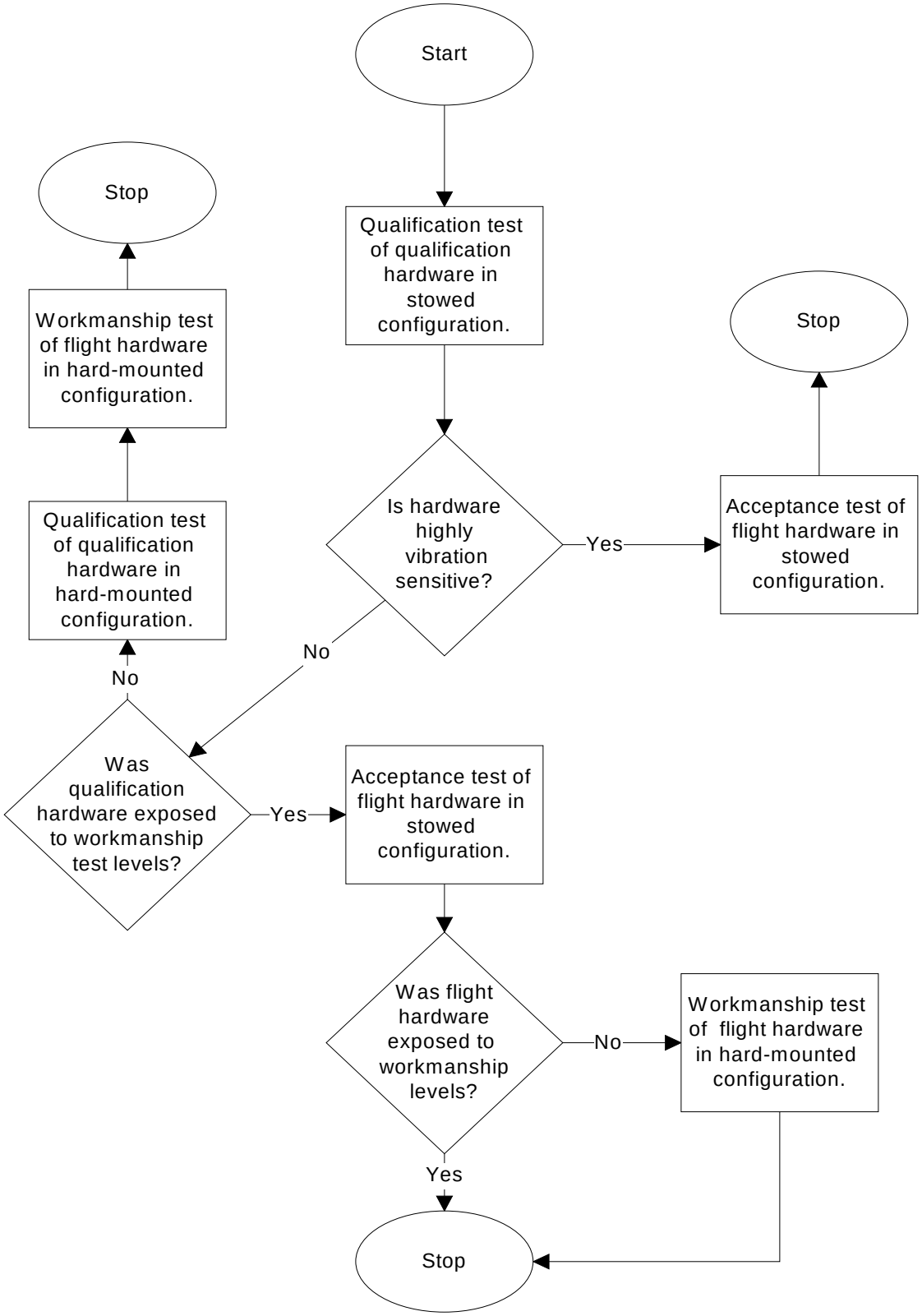

Figure 3.4-2—Vibration Testing of Stowed Hardware for Prototype Project.

3.4.9 Shock (Mechanical and Pyro)

a. The NASA-STD-7002 and NASA-STD-7003 ***shall*** be used for defining methodologies, practices, and requirements for verification of payloads and spacecraft to their shock environment.

b. Self-induced and externally induced shocks ***shall*** be considered in defining the shock environment. Self-induced shock occurs principally when pyrotechnic (explosive or propellant activated) and pneumatic devices are actuated to separate structural subsystems, deploy appendages, and activate onboard operational subsystems. Externally induced shock is produced by the operations of other subsystems. It is produced by either a mechanical or a pyrotechnic source. The shock experienced by a structure or hardware item is dependent upon the shock source type and strength, the intervening structure and discontinuities, and its distance from the shock source.

c. Pyroshock is typically characterized by its high-peak accelerations (up to 300 000 G), high-frequency content (up to 1 MHz) and short duration (less than 20 ms). Deformation or failure of major structures due to pyroshock is rare except in regions very close to the actual shock source. However, pyroshock can easily cause failures in small hardware items that are sensitive to high-frequency energy. These types of failures include relay and switch chatter; cracks and fractures in crystals, ceramics, epoxies, glass, solder joints, and wire leads; seal failure; and dislodging of contaminants resulting in short circuits. Verification of hardware to the shock environment is primarily done by testing.

d. Self-induced shocks typically result in testing at the system level (payloads, spacecraft, and large subsystems). Self-induced testing utilizes flight pyrotechnic/pneumatic devices and flight or flight-like intervening structure. As a result, duplication of the shock environment is reasonably achieved but a test magnitude margin is generally unachievable. For qualification and protoflight testing, it is recommended that a minimum of two firings be performed, to account for firing-to-firing variability. If acceptance testing is done on the flight article, only one firing is typical.

e. Externally induced shocks typically result in testing at the assembly level (electronic equipment, mechanical devices, components, and small subsystems). Externally induced testing is often performed using a controllable shock-generating device to simulate the shock at the hardware’s interface. The minimum statistic used to compute the flight limit level is P95/50. For qualification testing, a magnitude margin of 1.4 times the flight limit level is typically used and the testing repeated a minimum of two times per axis. For protoflight testing, the 1.4 magnitude margin is used but only one test per axis is performed. If flight acceptance testing is performed, no margin beyond the flight limit is used and only one test per axis is performed. (If it is not feasible to apply the shock with a controllable device, testing may be conducted at the payload level by actuating the shock-producing devices in the payload that produce the external shock to the subsystem to be tested. Two firings would be the minimum recommendation for qualification or protoflight testing.)

3.4.9.1 Flight Acceptance

a. The need for shock tests for the acceptance of previously qualified systems shall be considered on a case-by-case basis. Testing should be given careful consideration in accordance with mission reliability goals, shock severity, hardware susceptibility, design changes that could affect

proximity to the shock-producing device, and previous history. An end-to-end test of any pyrotechnic device shall be conducted for demonstration of acceptance for flight.

3.4.10 Mechanical Function

a. Mechanisms shall meet the requirements of NASA-STD-5017. A kinematics analysis of all mechanical operations shall be done. The analysis shall show that each mechanism can perform satisfactorily and have adequate design margins under worst-case conditions; satisfactory mechanical component clearances exist for stowed configuration, operational configuration, and any mechanical operation; and all mechanical elements are capable of withstanding the worst-case loads that may be encountered.

b. Verification tests are required to demonstrate that the installation of each mechanical device is correct and that no problems exist that will prevent proper operation of the mechanism during mission life.

3.4.10.1 Qualification Testing

a. Qualification tests of prototype/protoflight hardware are required for each mechanical operation at nominal-, low-, and high-energy levels. The nominal test ***shall*** be conducted at the most probable conditions expected during flight. High- and low-energy tests ***shall*** also be conducted to prove positive margins of strength and function. The levels of the tests ***shall*** demonstrate test margins beyond the nominal conditions to cover adverse interaction of potential extremes of parameters such as temperature, friction, spring forces, stiffness of electrical cabling or thermal insulation, and when applicable, spin rate. Parameters to be varied during these high- and low-energy tests ***shall*** include, to the maximum extent practicable, all those that could substantively affect the operation of the mechanism as determined by the results of analytic predictions or development tests. As a minimum, however, successful operation at temperature extremes 10°C beyond the range of expected flight temperatures ***shall*** be demonstrated.

3.4.10.2 Flight Acceptance Testing

a. Testing of mechanical mechanisms for proper operation is required only at the nominal condition with the required temperature extremes (see Section 3.4.10.1) for the acceptance of previously qualified systems. Mechanical mechanisms that are used for a fixed number of cycles ***shall*** be operated for at least one cycle but not greater than 10 percent of the intended number of duty cycles with no failures. For mechanical mechanisms that are limited life items, see Section 7.4.2.

3.4.11 Pressure Profile

a. The need for a pressure profile test ***shall*** be assessed for all subsystems. A qualification test ***shall*** be required if analysis does not indicate a positive margin at loads equal to those induced by the maximum expected pressure differential during launch and, if applicable, reentry. If a test is required, the limit pressure profile ***shall*** be derived from the predicted pressure-time profile for the nominal trajectory of the particular mission. The test ***shall*** be performed using the test factor for loads as specified in NASA-STD-5001. Because pressure-induced loads vary with the square of the rate of change, the qualification pressure profile is determined by multiplying the predicted pressure rate of change by the square root of the test factor of safety.

3.4.12 Fastener Integrity

a. Fastener integrity for space flight hardware is an area of concern because of the low MS often required to obtain acceptable system weight. For shuttle and ISS a fastener integrity plan is required as a Phase I safety submittal, while documentation of compliance with that plan is required as a Phase III safety submittal. A fastener integrity program must include activities to maintain fastener traceability, perform fastener testing (typically to verify chemical composition and strength), and provide controlled fastener storage.

b. The elements of the fastener integrity program must be tailored depending on whether the fasteners are fracture critical or not. For example, all fasteners should undergo lot testing to verify chemical composition, heat treat, strength, and lot variability. Fracture-critical fasteners, on the other hand, ***shall*** require NDE or proof testing of <u>each</u> fastener and ***shall*** require separate storage from the other fasteners.

c. Examples that can be used in developing a fastener integrity program include S-313-100 and JSC 23642.

3.4.13 Mass Properties

a. Mass is a critical attribute of space flight hardware and must therefore be budgeted and tracked throughout the life of the program/project. A weight budget must be defined early in the conceptual design phase to guide the design effort. Component and system mass properties are required as input to loads definition and strength analysis activities throughout the hardware development cycle. As-built mass properties must be verified by test before delivery of the hardware for flight. The International Society of Allied Weight Engineers (SAWE) can be a source of information on verification test methods.

b. Each space flight program must have a Mass Properties Control Plan and program. The mass properties to be tracked and controlled include weight (or mass), center of gravity (or center of mass), and sometimes, mass moments of inertia and products of inertia. The MIL-HDBK-1811 is an excellent guideline for establishing procedures for the control, determination, and documentation of mass properties of space flight hardware.

c. The following terminology is useful and should be used for all GRC flight programs/projects:

d. <u>Identified (or Basic) Mass Properties</u>. The identified mass properties of an item are the mass properties determined from an assessment of the most recent baseline design without including weight growth allowance. This assessment includes the estimated, calculated, or measured mass properties, and includes estimates for undefined design details (for example, fasteners or cabling). The weight growth allowance is not included.

e. <u>Weight Growth Allowance (or Contingency)</u>. The weight growth allowance is intended to cover uncertainty. It is the predicted increase of the mass properties of an item based on an assessment of the design maturity and fabrication status of the item, and an estimate of the design changes that may still occur. All space flight programs/projects ***shall*** make allowance for weight growth. Although there is no official standard for determining weight growth allowance, ANSI/AIAA G-020-1992 is available as a guide. The weight growth allowance may be applied at the system or the subsystem level (for an example, see Table 3.4-3). If the later approach is used, the subsystem contingencies may be rolled up using the RSS method if approved by the customer and the payload integrator. The program/project-specific Mass Properties Control Plan ***shall*** define and justify the weight contingencies to be applied throughout the program/project.

f. Predicted (or Current) Mass Properties. The predicted mass properties of an item are the identified mass properties plus the weight growth allowance. The predicted mass properties are the mass properties that must be compared to the budgeted mass properties. Worst-case mass properties must be used in strength and performance assessments. Usually the worst-case mass properties are the predicted mass properties, but in some cases, they may be the identified mass properties or even the budgeted mass properties.

g. Budgeted (or Control) Mass Properties. The budgeted mass properties are the limits imposed by the carrier or the system requirements and usually include a not-to-exceed weight and a center-of-gravity envelope. When predicted mass properties violate the budgeted mass properties, design modifications must be initiated to get the mass properties back within allowable values.

Table 3.4-3—Example of Weight Contingencies Applied
at the Component and Subsystem Level.
[For example, if the basic weight of structure during the conceptual
design phase is 200 lb, the predicted weight is 236 lb.]

Code	Design Maturity	Structure	Mechanisms	Wire & Cable	Batteries	Thermal Control	Electrical/Electronic Boxes and Components	10 lbs or less	Greater than 10 and no more than 30 lbs	Greater than 30 Lbs
E	Conceptual Drawings	18%	18%	33%	18%	18%	18%	18%	13%	8%
CL	Layout Drawings	13%	13%	18%	13%	13%	13%	13%	8%	3%
PR	Pre-released Drawings	3%	3%	8%	13%	8%	8%	8%	3%	3%
CR	Released Drawings	1%	1%	2%	2%	2%	8%	3%	3%	3%
A	Actual Weight	0%	0%	0%	0%	0%	0%	0%	0%	0%
S	Specification	0%	0%	0%	0%	0%	0%	0%	0%	0%

Note: Values are based on contractor's experience (used by LMSC on HST)

3.4.14 Ground Support Equipment

a. All ground support equipment (GSE) ***shall*** meet the requirements of NASA-STD-5005. In addition, the GSE for shuttle payloads ***shall*** meet the requirements of KHB 1700.7. All GSE to be used at the GRC ***shall*** also meet the requirements of the NASA Glenn Safety Manual.

b. In addition to the normal requirements for ground safety, transportation equipment must ensure that loads imparted to flight hardware during transportation and handling are no more than 80 percent of the design flight loads. Shock sensors are typically installed in shipping containers to record transient events during transportation and assure that design loads are not exceeded. If properly placed or denoted, the sensors can also serve as a deterrent to any rough handling by the transportation personnel. In some cases, the shock isolation capabilities of the shipping container may need to be verified by drop tests. Some guidance in shipping container drop testing can be found in NASA TM-86538.

3.5 Electromagnetic Compatibility (EMC) Requirements

a. Flight hardware is required to meet two basic criteria with regard to EMC. First, the equipment ***shall*** not generate and propagate electromagnetic energy which produces unwanted effects on its own mission objectives or the operation and safety of concurrently operating systems, that is, the launch vehicle, aircraft, or other flight hardware. Second, the equipment ***shall*** not be susceptible to the effects of electromagnetic energy within the defined mission environment. The electromagnetic interference (EMI) is the unwanted disturbance that affects an electrical circuit due to either conduction or radiation of electromagnetic energy from an external source.

b. Flight hardware ***shall*** meet the appropriate version of MIL-STD-461; Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment. The EMC ***shall*** be demonstrated by testing to the levels required by the program or project. A demonstration of 6 dB margins for safety-critical interfaces and a 20 dB margin for pyrotechnic circuits is typically required.

3.5.1 EMC Guidance

a. The goal of EMC is the correct operation of different equipment in a common electromagnetic environment. The EMC is achieved by controlling the unintentional generation, propagation, and reception of electromagnetic energy, and by hardening equipment against the effects of such energy. Two different kinds of issues must be considered to achieve EMC; emissions and susceptibility.

b. Emission issues are related to the unwanted generation of electromagnetic energy by various sources, and to the countermeasures, which are taken to reduce such generation and the escape of energy into the surrounding environment by conduction or radiation. Susceptibility issues refer to the unwanted effects on the operation of equipment in the presence of unplanned electromagnetic disturbances.

c. Programs and projects develop appropriate EMC requirements, which assure adequate margin exists between emissions and susceptibility of the payload and the conducted and radiated environment. This document does not present any GRC-unique EMI verification test levels or test methods since these requirements are dictated by programs and projects.

d. The EMC control plans are used to manage the process of achieving EMC through the control of EMI. The power distribution system, control functions, signal, data processing, and distribution functions must be managed through careful attention to electrical isolation, grounding, filtering, and shielding. It is important to recognize that EMI must be controlled in the time domain (in-rush current at turn on and turn off) and in the frequency domain (signal pass bands and switching power supplies).

e. Many experiments rely on the use of commercial off-the-shelf (COTS) equipment, which was not originally designed to comply with flight EMC requirements. The EMI control process must address how these noncompliant components will be managed in the integrated system such that the overall system will be able to achieve EMC.

f. Below are some design issues with COTS equipment:

g. Isolation—EMC specifications have a requirement for both power and signal isolation usually verified by a direct current measurement. These requirements are verified at the system level. Adherence to these principles within the system, while not mandatory in all cases, should not be

abandoned without sound engineering judgment. The most fundamental decision to be made for the power distribution system is whether to use a primary or secondary power distribution system and how this affects signal referencing. A system-level grounding and isolation diagram is useful for this purpose and ***shall*** be presented at, or prior to, the preliminary design review (PDR).

h. Bonding—The methods and processes of joining electrical faying surfaces, is specified as a method to assure an equal potential ground plane (at all frequencies) and to achieve electrical safety requirements. This requirement applies to all conductive materials unless a deviation is requested.

i. Shielding—Shielding may be employed to control radiated fields to and from the external environment (addressed by the verification requirements), and control of fields within equipment. Shields take the form of braids and foils for cables, and metal compartments within equipment. Shielding is normally applied to wiring connecting individual equipment or to reduce cable-to-cable coupling in signal circuits.

j. Filtering—Filtering may be employed to control conducted emissions into and out of individual equipment or components within equipment. The EMI control utilizing filtering is usually necessary to meet electrical transient requirements or limit the pass band of power, control, and signal circuits to meet emissions and susceptibility requirements. Filtering is best applied at the source of the unwanted interference. Twisted leads may help reduce electric fields.

3.6 Radiation Requirements

a. Electronic and optical components ***shall*** be verified through analysis or testing as being able to function in the expected ionizing radiation environment for the mission per the requirement of NPD 8730.2. The ionizing radiation environment effects include single event effects (SEE), total ionizing dose (TID), and displacement damage.

b. The TID is cumulative and dependent on the total number of events. Testing for TID is by a cobalt-60 gamma ray source per the method of MIL-STD-883 Method 1019 or an equivalent method using an ionizing radiation source such as high-energy protons. Device types susceptible to enhanced low dose rate sensitivity (ELDRS) undergo additional testing to characterize them for ELDRS if they are to be used in a low dose rate environment.

c. Displacement damage is also a cumulative effect. Testing for displacement damage in susceptible device types is by proton or neutron testing.

d. The SEE are quantitatively different from TID effects in that they are produced randomly. The purpose of SEE testing is to determine the MTBF of various electronic components. The SEE testing is accomplished through high-energy proton testing, heavy ion testing, or a combination of both. Components are monitored during exposure to determine when an error occurs, as well as what type of error. High-energy proton testing is less expensive than heavy ion testing. However, high-energy proton testing alone is less accurate than heavy ion testing and is used for programs and projects where higher risk is acceptable.

e. It is recommended that the components to be tested should be selected based on three criteria:

(1) System criticality: what would be affected by a subsystem failure?

(2) Development maturity: how flight-like is the hardware?

(3) Cost: In the event of part failure, how costly will it be to fix?

a. It is important to test items that are similar to the actual flight unit, where ‘similar’ is defined below:

(1) Both parts must be the product of the same approved qualified parts list, qualified manufacturer list, and/or ISO 9000 manufacturer.

(2) Both parts must have been manufactured on the same line.

(3) The processing of both parts must have been identical, especially the critical parameters of oxide growth, temperature of the oxide process, and final oxide thickness.

(4) The two parts must be similar in function and identical in technology including the same mask design and identical feature size, deposition, and doping.

(5) The same foundry, off shore or on shore, must have produced both wafers.

(6) Allowable technologies for radiation similarity consideration are the diffused metal oxide semiconductor (DMOS), complementary metal–oxide–semiconductor (CMOS), vertical metal oxide semiconductor (VMOS), diffused junction, and alloy junction.

b. Most likely, not all of these requirements can be met. Therefore, an alternative strategy of selecting and testing the same model number for a given component from the same manufacturer will provide confidence that the flight hardware will be representative of the units tested.

3.7 Vacuum, Thermal, and Humidity Requirements

a. Vacuum (if applicable), thermal, and humidity tests ***shall*** demonstrate that the system under test will

(1) Properly operate in the flight environment, specifically vacuum, temperature, and humidity.

(2) Properly control the thermal environment of temperature-sensitive items with a passive or active thermal control system.

(3) Survive the temperature and humidity conditions of transportation (e.g., truck, plane, space vehicle), storage, and pre and postlaunch conditions on the carrier.

b. These tests ***shall*** also act as an environmental screening to stimulate latent defects to maximize infant mortality.

3.7.1 Compliance with Requirements

a. The developer ***shall*** demonstrate compliance by conducting a set of tests and analyses that collectively meet the above requirements. Prior to conducting any test or analysis, the developer ***shall*** prepare a test and analysis plan that describes the methodology the developer will use to satisfy the requirements of this section. This plan ***shall*** be included as part of the review process, and the initial document reviewed no later than PDR.

3.7.2 Testing Levels

a. Test temperature range, margins, number-of-cycles, and humidity tests ***shall*** be determined using guidance provided in MIL-STD-1540, Test Requirements for Launch, Upper-Stage, and Space Vehicles.

3.7.3 Description of Applicable Testing

a. This section describes the minimum set of tests that are required to be performed to satisfy the requirements. Depending upon specific program/project requirements, additional tests may be required.

3.7.3.1 Thermal Cycling

a. Thermal cycling is a common testing method. It is used to verify thermal analyses, to verify acceptable performance over the operating temperature ranges, and to stimulate latent problems caused by manufacturing defects. Full functional tests ***shall*** be conducted during the first and last cycles. During the remaining cycles, the system under test ***shall*** be operated at least in its nominal functioning mode. The system under test ***shall*** operate failure free for the final three consecutive cycles.

3.7.3.1.1 Ambient Pressure Thermal Cycle

a. Systems under test that are designed/required to operate in vacuum or in microgravity environments not having forced convection, ***shall*** be subjected to the requirements of Section 3.7.3.1.2, "Thermal Vacuum." All other systems ***shall*** have thermal cycling performed at ambient pressure. Ambient pressure, as used here, means normal room environment and that a chamber capable of pulling vacuum is not required.

3.7.3.1.2 Thermal Vacuum

a. Thermal-vacuum tests are only required for systems under test that are designed/required to operate under a vacuum environment or in a microgravity environment where there is no forced convection cooling available. The thermal cycles ***shall*** be conducted at a vacuum level of 1.33×10^{-3} Pa (1×10^{-5} torr) or lower. Supplemental heating and cooling support systems (such as cold plates and chillers) will be required to condition the system under test.

3.7.3.2 Thermal Balance Testing

a. Thermal balance tests are used to verify and correlate the analytical thermal models of first-of-its-kind hardware so they may be used to predict hardware thermal behavior under flight conditions and to investigate scenarios where testing may be impractical. The adequacy of the thermal design and the capability of the thermal control system ***shall*** be verified under simulated onorbit worst case hot and worst case cold environments. Thermal balance testing is often performed in conjunction with thermal vacuum cycling, but it is preferable that the test precede the thermal vacuum test so that the results of the balance test can be used to establish the temperature goals for the thermal vacuum (cycle) test. Thermal balance tests ***shall*** be conducted at a vacuum level of $1.33\times10_{-3}$ Pa(1×10^{-5} torr) or lower.

3.7.3.3 Humidity

a. Humidity tests are only required for those systems that may be affected by humidity extremes which may be encountered during the life of the system.

3.7.4 Description of Applicable Analysis

a. There are many different methods to accomplish thermal analysis. The level of analysis needed will also depend upon the system being designed and built. As a minimum, all systems ***shall*** have a thermal analysis conducted that identifies the following:

(1) Heat sources and their magnitude

(2) Methods employed to dissipate the heat from the sources

(3) List of operating temperature ranges of the components

(4) Environmental conditions and design criteria

(5) An assessment of the thermal design and identification of additional analyses needed

(6) An evaluation of the susceptibility to humidity extremes

(7) Identification of any special testing requirements or conditions

b. This minimum analysis ***shall*** be completed and available no later than PDR.

3.8 Flight System Performance Acceptance Test Requirements

3.8.1 Burn-In Tests

a. For systems under test that contain electronic (EEE) parts, a burn-in is required to stimulate infant mortality failures. A minimum of 100 hours of failure-free operation is required. The 100 hours includes operational time accumulated during the thermal cycle testing and any functional testing. It is recommended that mission simulations be used to fulfill this time.

3.8.2 Mission Simulation Test

a. The mission simulation test is intended to demonstrate that the system will perform the total set of operations it was designed and programmed for in a simulated flight environment. The program/project ***shall*** perform a mission simulation prior to flight using the flight system (hardware and software). This simulation would cover all nominal operations and functions, and if appropriate, contingency cases. The system operation ***shall*** simulate the real flight mission operations as closely as possible. This would include using external stimulus or instruments, simulation of external signals, data flows, and external system control.

3.8.3 End-to-End Compatibility Test

a. The end-to-end compatibility test is intended to demonstrate the compatibility of the system with other mission operational elements. The end-to-end requirements apply equally to the testing of prototype flight payloads or the testing of previously qualified system. An end-to-end compatibility test ***shall*** be conducted on the complete operational system in the final mission configuration, as closely as possible. This test would include the flight system, the flight operational software, the carrier/carrier simulator, and the mission operations system, including the ground processing equipment and software in order to fully demonstrate operational compatibility and the ability of the entire system to perform as required during the mission. The carrier or program available systems necessary for this test ***shall*** be requested and addressed in the Integration Plans and Agreements.

Chapter 4. System Safety

4.1 Introduction

a. System safety is a disciplined, systematic approach to the analysis of risks resulting from hazards that can affect humans, the environment, and mission assets. It is a critical first step in the development of risk management (RM) strategies. System safety covers the total spectrum of technical risk and management activities including safety and risk assessments and safety performance monitoring.

b. This section is intended to flow down requirements from NPR 8715.3 for system safety applicable to space programs or space projects managed by GRC.

4.2 System Safety Planning

a. Every program/project ***shall*** develop a System Safety Technical Plan (SSTP). The SSTP is designed to be a technical planning guide for the technical performance and management of the system safety activities. The SSTP can be a standalone document, or part of the SMAP or the Systems Engineering Management Plan (SEMP). It provides the specifics of the system safety modeling activities and describes what and how safety adverse consequences will be modeled, how system safety models (qualitative and probabilistic risk assessments) will be integrated and applied for risk-informed decision making and safety monitoring, how the technical team(s) responsible for generating and maintaining system safety models will interact with the system engineering organizations, the reporting protocol, and the resources and schedule associated with accomplishing system safety modeling activities in relation to the critical or key events during all phases of the life cycle.

4.2.1 System Safety Assurance Reviews

a. The approach used to comply with the system safety requirements will be an agenda item at each of the program/project reviews, as such, the GRC reviews will complement the system safety reviews. Each program/project ***shall*** institute a rigorous system safety program beginning with the conceptual phase of the element. System safety requirements ***shall*** be an integral part of all technical developments and as such will be an agenda item at each of the reviews listed above. The purpose of the system safety reviews is to evaluate the status of system safety and risk analysis, RM, verification techniques, technical safety requirements, and program implementation throughout all the phases of the system life cycle.

b. There are typically four phased safety reviews for programs/projects in accordance with the various safety requirements. These are nominally Phases 0, 1, 2, and 3, which are associated typically with a program/project’s conceptual design review, preliminary design review (PDR), critical design review (CDR), and preship review (PSR), respectively. For many programs/projects, the phased safety reviews are sometimes combined depending on the complexity of the program/project. The GRC Safety and Mission Assurance Directorate (SMAD) should be consulted if a program/project wishes to combine reviews. In addition, safety requirements for some programs/projects require separate flight and ground phased safety reviews, for example, shuttle and/or International Space Station (ISS) payloads. Refer to the applicable safety requirements referenced in Chapter 8 for the need for separate flight and ground safety reviews.

4.3 Hazards Analysis

a. Hazards analysis involves the application of systematic and replicable methods to identify and understand hazards, and to characterize the risk of mishaps that involve hazards. There are several types of hazard analysis that include Preliminary Hazard Analysis (PHA), System Hazard Analysis (SHA), Subsystem Hazard Analysis (SSHA), Functional Hazard Analysis (FHA), Operating and Support Hazard Analysis (O&SHA), Software Hazard Analysis (SWHA), and Integrated Hazard Analysis (IHA). The required use of one or more of these hazard analyses or others ***shall*** be defined in the SSTP. Hazard analysis may also identify methods/strategies to mitigate identified hazards in a system. The following is the order of precedence of methods/strategies that ***shall*** be used to mitigate hazards:

(1) Eliminate the hazard.

(2) Incorporate safety devices that may reduce the likelihood of occurrence of a mishap from the associated hazard or reduce the severity of the mishap consequences.

(3) Provide caution and warning devices.

(4) Develop and implement special procedures including the use or personnel protective equipment.

b. The use of more than one of these mitigation methods/strategies in combination may be required to mitigate a hazard to an acceptable level of risk.

4.4 Failure Tolerance

a. Failure tolerance is a fundamental system safety approach to controlling hazards by the incorporation of redundant systems into the design of the system. The goal of this redundancy is to reduce the likelihood of occurrence of a mishap from the associated hazard. Failure tolerance is defined by levels depending on the amount of redundancy. A zero failure tolerance design has no redundancy for controlling a specific hazard. A single failure tolerance design has a single level of redundancy for controlling a hazard. A two failure tolerance design has two levels of redundancy for controlling a hazard. The level of failure tolerance required to control a hazard is usually commensurate with the severity of the hazard in question. Failure tolerance requirements including the associated verification requirements are defined to the applicable governing safety document(s) that are listed in Section 4.9., Implementation of Failure Tolerance, does not alleviate the need to prevent failures.

4.5 Design for Minimum Risk

a. Design for minimum risk (DFMR) is a fundamental system safety approach to controlling hazards that is an alternative to failure tolerance. It is typically used when failure tolerance is not practical and involves applying a design margin to a system. The means for determining design margin must be well understood and verifiable. Examples of DFMR solutions include applying factors of safety for primary structure, pressure vessels walls, and pressurized lines. The DFMR requirements including the associated verification requirements are defined to the applicable governing safety document(s) that are listed in Section 4.7.

4.6 Internal GRC Review of Safety Products

a. All GRC developed or sponsored safety products, for example, Safety Data Packages and System Safety Analysis Reports, are required to be reviewed and approved/concurred by the SMAD.

4.7 Requirements Applicability

a. The following table provides the applicable safety requirements document for each type of flight hardware being developed. Additional safety requirements documents may be referenced within these top-level documents.

Hardware Classification	Governing Safety Document(s)
Constellation	CxP 70038
Shuttle Payload	NSTS/ISS 13830C, NSTS 1700.7, KHB 1700.7
ISS Payload	NSTS/ISS 13830C, NSTS 1700.7 ISS Addendum, KHB 1700.7
Shuttle Detailed Test Objective	NSTS 16725
ISS Detailed Test Objective	SSP 50448
Shuttle Government Furnished Equipment	JSC 17481
ISS Vehicle Hardware	SSP 30309, SSP 50021
Expendable Launch Vehicle Payload	NPR 8715.7
Automated Transfer Vehicle Payload	ESA-ATV-PR-13830, ESA-ATV-1700.7
Progress and Soyuz Payloads	P32928-103
Ariane Payload	CSG-RS-10A-CN, CSG-RS-21A-CN, CSG-RS-22A-CN
Japanese H-IIA Payload	NASDA-ESPC-2857

Note: Payloads flown on an Expendable Launch Vehicle, the Automated Transfer Vehicle, or Progress to the ISS for operations there ***shall*** also meet the ISS Payload Safety Requirements.

Chapter 5. EEE and Mechanical Parts Control

5.1 General Requirements

a. The program/project ***shall*** plan and implement an electrical, electronic, electromechanical (EEE), and mechanical parts control program according to the general guidelines of NPD 8730.2 that complies with the requirements as outlined in this section. The parts control program implemented ***shall*** support the required mission life and environment. Parts ***shall*** be selected and controlled based on performance, environmental (ground and flight), criticality for safety and mission success, and lifetime requirements. The requirements of this section ***shall*** apply to all flight system fidelities including qualification and protoflight systems.

5.2 EEE Parts Selection and Screening

a. The EEE parts (capacitors, circuit breakers, connectors, crystals, discrete semiconductors, filters, fuses, hybrids, inductors, microcircuits, photonics, relays, resistors, switches, transformers, wire and cable, etc.) ***shall*** be selected in order to meet program/project reliability and availability requirements over mission life. In addition, parts selection ***shall*** be driven by safety requirements, performance requirements, worst-case environmental conditions (e.g., radiation, thermal, atomic oxygen, vacuum, and vibration), and maintenance allocations defined by the equipment specification.

5.2.1 EEE Parts Control Plan

a. An EEE parts control plan ***shall*** be identified in the Safety and Mission Assurance Plan (SMAP). This plan can be either a standalone document or part of the SMAP. The plan ***shall*** be established to verify and certify that the electrical form, fit, and function of EEE parts meet program or program/project requirements, and to protect against counterfeit or noncompliant parts. The plan ***shall*** control parts selection, qualification, screening, de-rating, radiation hardness requirements and other environmental constraints, parts list and traceability requirements, incoming inspection, storage and handling, prohibited materials, and any other requirements necessary to meet mission objectives. Additional guidance in developing the EEE parts control plan can be found in GLHB-QE-8730.1 and the relevant documents within GLM-QE-8700.1.

5.2.2 EEE Parts Selection and Grade

a. The EEE parts control plan ***shall*** specify the grade level of parts to be selected. The grade level of a given part is related to the associated risk, with the highest-grade parts (e.g., Grade 1 or Class S) having the lowest risk. Higher grade parts will have higher reliability due to the manufacturer’s quality assurance procedures and practices, including screening. Parts manufactured on a qualified manufacturing line will tend to be the most reliable. Parts ***shall*** be considered to have low, medium, high, or unknown risk as described in the EEE Parts Risk Assessment Matrix (GLHB-QE-8730.1, Appendix C). For commercial and industrial parts, the risk is unknown and must be assessed on a case-by-case basis. Commercial and industrial parts are usually of higher risk than qualified military parts.

b. Programs or projects requiring higher grade or lower risk parts ***shall*** have a standard (or preferred) parts list. Parts to be used in flight hardware ***shall*** be selected from the standard parts

list as much as possible. Parts not on the standard parts list ***shall*** be considered nonstandard and ***shall*** require review and approval before use in flight hardware.

c. The NASA Parts Selection List (NPSL) has been developed to serve as a parts selection tool for NASA space flight programs. In general, parts listed in the NPSL have established procurement specifications, have available source(s) of supply, are capable of meeting a wide range of application needs, and have been assessed for quality, reliability, and risk. Parts listed in the NPSL ***shall*** be used in space flight hardware when they meet the program/project's needs and ***shall*** be considered for inclusion in standard or preferred parts lists.

5.2.3 Flight EEE Parts Qualification

a. The EEE parts used in high-reliability flight hardware ***shall*** be qualified to verify that materials, design, performance, and long-term reliability of the parts are consistent with the specifications and intended applications. Parts procured to military specifications ***shall*** be from manufacturers listed on the qualified parts list or qualified manufacturers list for the specification. Nonmilitary specification parts ***shall*** be qualified per an approved source control drawing, the qualification methods of EEE-INST-002, or an approved qualification plan. Parts used in an application requiring a higher grade level ***shall*** be qualified for that grade level.

5.2.4 Flight EEE Parts Screening

a. The EEE parts used in flight hardware ***shall*** be subjected to screening to remove nonconforming parts from an otherwise acceptable lot of parts or to reject unacceptable lots. Screening for parts used in high-reliability applications ***shall*** be at the piece part level and ***shall*** follow the requirements of the appropriate military or NASA specification, an approved source control drawing, or an approved screening plan.

b. Additional screening is required when a part of higher or unknown risk is used in an application requiring lower risk parts. The additional screening ***shall*** meet the requirements of EEE-INST-002. The developer may adopt their own upgrade screening requirements with GRC approval.

c. Screening at the piece part level is not required for low budget projects, which are typically short duration (0 to 14 days) (excluding man-rated launch vehicles). These are projects for which high reliability is not an important factor, the mission is not critical, and mostly parts of high or unknown risk including commercial and industrial parts are used. Also, screening individual parts is not practical for commercial off-the-shelf assemblies. Instead of screening at the piece part level, the following tests ***shall*** be performed at the assembly or system level:

(1) Burn-In (see Section 3.8.1)

(2) Thermal Cycle (see Section 3.7)

(3) Vibration (see Section 3.4.8)

5.2.5 De-rating

a. The de-rating of parts improves the reliability of systems (reference Preferred Reliability Practice PD-ED-1201). All EEE parts ***shall*** be used in accordance with the de-rating requirements and guidelines of GLM-QE-8730.1. Another NASA de-rating document or a developer's de-rating policy may be used instead of the above if it has received GRC approval.

5.2.6 Radiation Hardness

a. Parts ***shall*** be selected so that flight hardware meets all performance and reliability requirements under exposure to the predicted radiation environment, including total ionizing dose effects, displacement damage, and single event effects. Guidance on designing for the radiation environment and sources of parts radiation data can be found in GLWI-QE-8730.6.

5.2.6.1 Total Ionizing Dose

a. Parts ***shall*** be selected so as to not exhibit malfunction or degradation of performance beyond specified tolerances when exposed to the total dose ionizing radiation environment. Total dose damage is cumulative and is a function of time, exposure, and shielding. As time of exposure increases and shielding decreases, the absorbed total dose will increase. The expected total dose ***shall*** be defined for each mission.

b. The program/project ***shall*** demonstrate through testing or analysis whether the selected parts can withstand the expected total dose. Testing may be performed at the assembly level under nominal bias conditions and at the expected flight environment dosage. Use of parts without total dose testing is normally acceptable when total dose is less than 1 krad (Si).

c. Alternatively, in lieu of testing, an analysis of the parts list ***shall*** be performed. The expected dose may be compared to the susceptibility of semiconductors and microcircuits in the parts list.

5.2.6.2 Single Event Effects

a. Parts ***shall*** be selected so that equipment meets specified performance requirements when exposed to the single event effects (SEE) radiation environment. The SEE include single event upsets, transients, latch-ups, burnouts, gate ruptures, and snapbacks. Safety-critical circuits ***shall*** be designed so that they will not fail because of SEE.

b. The likelihood of SEE occurring is a function of the sensitivity of the device in question and of the natural space environment that will be encountered. Unlike total dose, SEE is not a cumulative effect; it does not depend on the length of time in orbit. The developer ***shall*** demonstrate through testing (see Sections 3.6.1 and 3.6.2) or analysis whether the selected parts can withstand SEE. Proper part selection, as well as appropriate circuit design and parts de-rating, can help to mitigate the impact of SEE, and designers ***shall*** compare their parts lists to existing test data.

5.2.6.3 Displacement Damage

a. Parts ***shall*** be selected so as to not exhibit malfunction or degradation of performance beyond specified tolerances due to displacement damage resulting from ionizing or nonionizing radiation. Displacement damage is cumulative. Evaluation of susceptibility to displacement damage ***shall*** be through testing or analysis.

5.2.7 Corona and Arcing

a. All unsealed electrical and electronic components, which are required to operate during ascent/descent, in a vacuum environment, or during a depressurization or repressurization event ***shall*** be tested for corona and arcing during thermal vacuum testing (see Section 3.7.3.1.2 and reference MSFC-STD-531, Preferred Reliability Practices PD-ED-1202 and PT-TE-1415).

5.2.8 Inspection Prior to Assembly

a. The EEE parts ***shall*** be inspected prior to their assembly into flight systems or subsystems to ensure they are free of any debris, defects, or other manufacturing faults that would interfere with their form, fit, and function. The EEE parts that are safety or mission critical ***shall*** be tested to verify and certify their electrical performance and to protect against counterfeit or noncompliant parts prior to assembly into flight systems or subsystems.

5.3 Mechanical Parts Selection and Screening

a. Mechanical parts ***shall*** be selected in order to meet program/project reliability and availability requirements over mission life. To the greatest extent possible, selection of mechanical parts (fasteners, bearings, studs, pins, shims, valves, springs, slides, pulleys, brackets, clamps, spacers, etc.) ***shall*** be made from previously qualified parts that meet space flight performance, environmental, criticality, and life cycle requirements.

b. In selecting mechanical parts, the material compositions must be addressed as defined in Chapter 6 and ***shall*** be addressed for life cycle use. Specific attention should be given to any lubricants, sealants, coatings, and other materials and processes that are utilized by the vendors, and their acceptability for the planned environment and life cycle use. Many commercial lubricants are unacceptable for space flight applications due to offgassing, outgassing, or their physical behavior in microgravity.

5.3.1 Mechanical Parts Control Plan

a. A mechanical parts control plan ***shall*** be identified in the SMAP. This plan can be part of the fracture control plan (see Section 3.4.5) or can be a standalone document. The plan ***shall*** be established for mechanical parts that are part of the primary structural load path to verify and certify their structural strength and materials and to protect against counterfeit or noncompliant parts. Fastener control ***shall*** address lot testing for structural strength and material composition and storage and use control.

5.3.2 Inspection Prior to Assembly

a. All mechanical parts ***shall*** be inspected prior to their assembly into flight systems or subsystems to ensure they are free of any debris, defect, or other material or substance that would interfere with their function. All mechanical parts that provide rotational, transitional, or other movements ***shall*** be tested for full range of motion, and inspected for freedom of motion (resistance) prior to assembly into flight systems or subsystems.

5.4 Procurement of Parts

a. Parts ***shall*** be procured directly from the manufacturer or from the manufacturer's authorized or franchised distributor. Parts may be purchased from independent distributors or brokers only when this is unavoidable, provided measures are taken to mitigate the risk of receiving counterfeit or discrepant parts.

b. Procurements ***shall*** clearly identify the specification for items being purchased and ***shall*** request certification of conformance to the required specifications. Procurement of parts ***shall*** be coordinated among programs and centers whenever feasible. Surveys and audits ***shall*** be utilized to determine whether suppliers meet program or project requirements.

5.4.1 Parts Obsolescence and Diminishing Manufacturing Sources

a. Consideration ***shall*** be given in parts selection and procurement to ensuring parts availability for repair and new builds throughout the projected life of the equipment. Parts that are inactive for new design ***shall*** not be selected and obsolete parts or parts scheduled to be discontinued ***shall*** be avoided for new designs. Sufficient parts ***shall*** be procured to support maintenance and planned or potential future builds.

b. Any program or project of sufficient duration that it could be negatively impacted by parts obsolescence ***shall*** maintain a process for monitoring their parts for and mitigating the effects of parts obsolescence.

5.5 Parts Storage Control

a. Parts ***shall*** be stored in a bonded storage area as defined in Section 8.6.4.

5.6 Parts Age Control

a. As some types of parts may fail or drift while in storage, parts assemblies ***shall*** be subjected to functional retest and recalibration prior to flight. The program/project verification plan ***shall*** contain the details of the calibration sensitive items and their required calibration cycle. If there is any system modification because of a failure during the acceptance test, the functional acceptance test ***shall*** be repeated. In addition, if there is a significant system modification that may affect the mechanical/software integrity of the assembly, the thermal cycle and vibration procedures of the acceptance test ***shall*** be repeated.

5.7 Parts Identification List

a. A Parts Identification List (PIL) for EEE and mechanical parts ***shall*** be prepared, maintained, and updated by the program/project in accordance with the program/project's configuration control system. All submissions to the GRC PM and Chief Safety and Mission Assurance Officer ***shall*** be in a computer-readable form. The PIL ***shall*** be reviewed against Government-Industry Data Exchange Program (GIDEP) Failure Experience Data and NASA Parts Advisories (see Section 8.10).

b. The PIL ***shall*** be compiled by program/project component, instrument, or instrument component and ***shall*** include as a minimum the following information: part number, part name or description, manufacturer name or Commercial and Government Entity (CAGE) number, quantity, drawing number, and name of the next higher assembly where part is located. The part number ***shall*** be the part number to which the part is procured, which will be the military specification part number if it is a military part, a source control drawing (SCD) part number if it is manufactured to the requirements of such a drawing, or the manufacturer’s part number.

c. The program/project ***shall*** create and maintain an as-designed parts list (ADPL) and an as-built parts list (ABPL). The ADPL lists the parts that are intended for use in the flight equipment. The ABPL is a list of the actual parts assembled into the flight equipment and becomes part of the Acceptance Data Package.

d. The program/project ***shall*** maintain traceability by part number, manufacturer, screening serial number, and lot date code for all parts assembled into flight hardware through the use of configuration identification lists (build paper) (see Section 8.4).

5.8 Parts Risk Evaluation

a. The risk associated with each part ***shall*** be evaluated according to Section 5.2.1 and 5.3.1 and based on program/project requirements. Lower risk parts and backup components (sparing) ***shall*** be used to meet the program/project availability goal. The risks involved with using parts with medium, high, or unknown risks ***shall*** be defined through individual or team uncertainties, program/project data, analysis, or tests. The risks ***shall*** be mitigated or accepted, tracked, and controlled through the continuous risk management process (see Chapter 9).

5.9 Parts Subject to Metal Whisker Growth

a. The use of parts plated with pure tin, zinc, cadmium, or other metals that are subject to the growth of metal whiskers ***shall*** be avoided in applications where the whiskers may cause electrical short circuits, plasma arcing in vacuum, or contamination. If such parts must be used, measures ***shall*** be taken to mitigate this risk.

Chapter 6. Materials and Processes Requirements

6.1 General Requirements

a. This section establishes the materials and processes requirements for the design, fabrication, and testing of flight components for all NASA manned, unmanned, robotic, launch vehicle, lander, in-space and surface systems, and spacecraft program/project hardware elements. All flight hardware is covered by the materials and processes (M&P) requirements of this document, including vendor/subcontractor-designed, off-the-shelf, and vendor/subcontractor furnished items. Programs, projects, and elements are responsible for contractually levying these requirements down through every tier of hardware developer, to the lowest component-level suppliers. These requirements provide a common framework for materials and processes control practices on all NASA programs. Programs/projects ***shall*** be responsible for demonstrating compliance with these requirements.

b. The NASA-STD-6016 ***shall*** be used as the minimum requirements for materials and process selection, implementation and control, and provides a general control specification for incorporation in NASA program/project hardware procurements and technical programs.

c. The cornerstone of NASA-STD-6016 is the required materials and process selection, control and implementation plan (also known as the M&P Plan). This M&P Plan provides the program/project the opportunity to tailor the degree of conformance and describe the method of implementation for each requirement identified in NASA-STD-6016.

d. When the M&P Plan has been approved by the responsible contractual M&P authority, as an acceptable means of compliance with the technical requirements, the plan replaces the NASA-STD-6016 requirements obligation and becomes the programmatic M&P requirements document. Small projects or simple deliverables can embed their M&P Plans in the Safety and Mission Assurance Plan (SMAP), and the SMAP is signed by the responsible contractual M&P authority. Complex projects require standalone M&P Plans. A higher tier project can impose their in-house M&P Plan on a lower tier, require the lower tier to draft a specific M&P Plan, or allow the M&P details to be embedded in a related document, as long as the M&P review and approval authority is traceable.

e. The approved M&P Plan may be used for the implementation and verification of M&P requirements on the applicable program/project. Note that Section 4.3 of NASA-STD-6016 explicitly describes what tangible verification activities are expected in satisfaction of NASA-STD-6016 or the governing M&P Plan requirements. Numerous "***shall***" statements are found throughout all of the sections of NASA-STD-6016, but are not expected to be addressed as individual verification items. The governing M&P Plan can address how verification is to be accomplished.

f. In addition to the M&P Plan, examples of typical deliverables that are reviewed and approved by M&P are found in NASA-STD-6016 and include the nondestructive evaluation plan, contamination control plan, material usage agreements, and materials identification and usage lists.

g. Additionally, at a minimum, regardless of whether the developer's M&P Plan is standalone or incorporated into the SMAP, the program/project's SMAP ***shall*** define the general approach,

roles, and responsibilities the program/project expects to apply to meet the M&P requirements. Roles and responsibilities include definition of who is the responsible contractual M&P authority and how the approval cycle functions.

h. For GRC in-house programs/projects the Business Management System (BMS) procedures that apply can be found in the reference documents list.

6.2 Safety and Mission Assurance Plan Specific Requirements

a. The SMAP ***shall*** address how M&P control will be accomplished by the program/project. This ***shall*** include, but is not limited to:

(1) Organizational roles and responsibilities for meeting the programmatic M&P requirements. The hierarchy of approval authority for program/project M&P documentation ***shall*** be established and documented in the SMAP. Approval authority is program/project specific. This is tied to organizational roles and responsibilities and clarifies what M&P entities have approval and oversight authority.

(2) The SMAP ***shall*** document the general approach to M&P controls through each tier of responsibility, both downward and upward. This would outline whether a standalone M&P Plan is expected and expound on how the M&P Plan or NASA-STD-6016 requirements are passed along through the tiers.

(3) The SMAP ***shall*** document the responsibilities of the program/project M&P engineer and the PPAD M&P engineer, including description of specific insight/oversight activities or direct drawing signoff responsibility. Activities for in-house programs/projects, contractor led or supported programs/projects, and programs/projects sponsored by other Centers will vary widely on their approach to M&P responsibility.

(4) The Shuttle and international space station payloads will continue to recognize the GRC Materials Certifying Official as the M&P approval authority, as referenced in GLP-8730.8, Materials and Processes, and other BMS documents.

(5) If the program/project desires to embed the M&P Plan within the SMAP, then a much more extensive technical discussion of the M&P requirements and implementation is expected. Approval by the M&P governing authority would then be required on the SMAP.

(6) Requirements for fracture control are not addressed by the SMAP or NASA-STD-6016. Fracture Control for flight hardware structure, including pressure vessels, is implemented by GLPD 1150.3 and programmatic fracture control requirements documents.

Chapter 7. Reliability and Probabilistic Risk Assessment

7.1 Reliability, Availability, and Maintainability

a. This section is intended to flow down requirements from NPD 8720.1 and NPR 8715.3 for reliability, availability, and maintainability (RAM) applicable to Space programs or Space projects managed by GRC.

7.1.1 General Requirements

a. The RAM program will identify the requirements, activities, and resources needed to assure that system design meets the required level of RAM as determined by the program or project. The RAM disciplines will verify through analysis and review of testing that the system design meets RAM requirements. The following table summarizes some of the RAM requirements for space programs/projects.

RAM Requirements Summary Table for Space Programs/Projects

Requirements	Method of Verification
System RAM Design performance requirements Qualitative • Failure Tolerance Requirement • Protection from Failure Propagation • Fail-Safe • Separation of Redundant Paths • Health status and monitoring Capability • Failure Detection, Isolation & Recovery (FDIR) • Functional verification of Systems Quantitative • System Reliability • Subsystem (or Functional) Reliability Allocations • Expected Operating and Storage Life	Qualitative • Failure Modes & Effects Analysis (FMEA) • Critical Items List (CIL) and Retention Rationale • Fault Tree Analysis (FTA) • System Functional flow Block Diagrams Quantitative Reliability Allocation Reliability Modeling and Analysis Fault Tree Analysis Limited Life Items List and Plan
System RAM operational performance requirements Qualitative • System Survival in intended Mission Environment Quantitative • Maintainability and Availability Allocations Examples are: - Mean-time-to-Restore, Repair, or Replace (MTTR) - Mean Administrative Delay Time - Mean-Logistics-Delay Time - Mean-time-Between Maintenance Actions (MTBMA) - Cumulative Corrective Maintenance Time - Operational Availability	Qualitative • Environmental Stress Screening Quantitative • Maintenance Task Analysis • Maintainability Analysis • Operational Availability Analysis
• System Maintenance Concept	• Maintainability Concept Document • Corrective and Preventative Maintenance Plans
• RAM Engineering Tasks	• RAM Program Plan
• Assessment	• Progress toward achieving RAM requirements at milestone reviews • Identification of areas for improvement in RAM reporting
• Integration of RAM processes	• Business Management System (BMS) Work instructions for RAM processes include a flow of information and review between RAM engineering, and SMA disciplines.

7.1.2 Requirement for and Integrated Process

a. The RAM processes and analytical activities ***shall*** be integrated with the design and development process, systems engineering, RM, safety, QA, software assurance (SA),

Probabilistic Risk Assessment (PRA), and logistics. All disciplines will provide information, data, and participation with RAM engineering to plan, establish, document, and implement a RAM program.

b. The RAM program ***shall*** encompass the following areas:

(1) System RAM design and operational performance requirements (qualitative and quantitative)

(2) System maintenance concepts

(3) Requirements and tasks for RAM engineering and analysis

(4) Review of testing

(5) Software, firmware, and human-induced faults

(6) Assessment of progress toward achieving RAM requirements and identification of areas for improvement

c. The program/project systems engineering and components engineering groups ***shall*** respond to qualitative and quantitative RAM requirements and analysis by addressing design areas where RAM improvement is needed. Information required to update RAM models and analyses will be provided by systems and components engineering. In particular, program or project engineering groups will respond to the Critical Items List (CIL), derived from the Failure Modes and Effects Analysis (FMEA) by designing single point failures or providing data and other information required to develop retention rationale. The program/project will participate in the development of the CIL and its retention rationale. This process ***shall*** be supported over the course of the program or project.

7.1.3 RAM Management

a. Each Space Program/Project ***shall*** implement a RAM program to support their development and operational phases unless there is a specific approved waiver to this activity. The PMs and the SR&QA managers ***shall*** manage the RAM program. The RAM engineering will be tracked for progress against each major milestone goal. At major milestone reviews, progress toward achieving the reliability requirements, including identification of areas for improvement will be provided.

7.1.4 RAM Plan

a. The PMs and the Safety, Reliability and Quality Assurance (SR&QA) managers ***shall*** ensure that a RAM plan is prepared and tailored in order to apply to a specific program or project. The plan ***shall*** address the requirements specified in this document for RAM. The RAM effort for each program/project ***shall*** be governed by the plan that will be contained in the program or project's Safety and Mission Assurance Plan (SMAP). If specific requirements do not apply to a program/project or will not be implemented for various reasons, the requirement area is documented in the SMAP as "not planned" and with a substantiating rationale and approval by management.

7.1.5 RAM Data

a. The PMs ***shall*** provide and maintain RAM data from test, prelaunch, flight, and recovery for use as heritage data. The Center Safety and Mission Assurance (SMA) functional manager is responsible for usage of RAM data in RAM analyses.

7.1.6 RAM Reports Archives

a. The program/project's configuration management system ***shall*** maintain an archive of all RAM reports developed for the program or project. The Program and Project Assurance Division ***shall*** maintain a backup archive of all RAM reports developed for the program/project.

7.1.7 Reliability and Failure Tolerance

a. Safety-critical systems ***shall*** have a high reliability as specified in the program/project system reliability requirement and resulting functional allocations (derived from NPR 8715.3). The NPR 8715.3 states that if high reliability cannot be verified by reliability analysis using accepted modeling techniques and accepted data with a specified confidence level, then the following items ***shall*** apply:

(1) Safety-critical systems ***shall*** be designed to have failure tolerance and safety margins.

(2) Safety-critical systems ***shall*** be designed so that no combination of two failures and/or operator errors will result in loss of life (fail-safe as a minimum).

(3) No single failure or operator error will result in system loss/damage or personnel injury.

(4) System design must provide functional redundancy in those cases where there is insufficient time for recovery or system restoration.

b. However, failure tolerance requirements for man-rated systems ***shall*** apply regardless of the results of reliability analysis. Any program failure tolerance requirements ***shall*** apply regardless of the results from reliability analysis.

c. Where there is sufficient time between a failure and the manifestation of its effect, design for restoration of safe operation using spares (removal and replacement), repair, or operational procedures, provides an acceptable alternative to failure tolerance (derived from NPR 8715.3).

d. Safety-critical systems and operations ***shall*** be designed to have a safety margin.

e. When using redundancy, the program/project ***shall*** verify that common cause failures (e.g., contamination, close proximity) do not invalidate the assumption of failure independence. Common cause failures will not defeat the redundant design.

7.1.7.1 Variances from Two-Failure Tolerance Requirement

a. When requesting a variance from the two-failure tolerance requirement, the program/project ***shall*** provide evidence and rationale that (1) Two-failure tolerance is not feasible for technical reasons, (2) The system or subsystem is designed and certified in accordance with approved consensus standards.

7.2 Probabilistic Risk Assessment (PRA)

7.2.1 General Requirements

a. This section is intended to flow down requirements from NPR 8705.5 for PRA applicable to space programs or projects managed by GRC.

b. The continuous risk management program ***shall*** propose the level at which PRA ***shall*** be conducted. The proposal will be discussed with the PM, and the program or project will arrive at a decision (the PRA decision). The PRA decision and its basis ***shall*** be documented in the

program or project RM plan. Disputes concerning the PRA decision and level of implementation ***shall*** be elevated to the next higher level of program management.

7.2.2 Criteria for PRA Decision

a. A “full-scope” analysis contains all major PRA components as outlined in Chapter 2 of NPR 8705.5. Full-scope PRA ***shall*** be performed for systems supporting manned space flight, nuclear payloads, launch vehicles, mars sample return missions, and human space experiments.

b. A “limited-scope” PRA applies the steps outlined in Chapter 2 of NPR 8705.5. with the same general rigor as a full-scope PRA, but focuses on a smaller set of the mission-related end states of specific decision-making interest, instead of all applicable end states. A limited-scope PRA may be performed on Earth Science Missions, Space Science Missions, and technology demonstrations.

c. A “simplified PRA” contains a reduced set of scenarios or simplified scenarios designed to capture only essential, sometimes top level, mission risk contributors. A simplified PRA may be performed on Earth Science Missions, Space Science Missions, and technology demonstrations.

7.2.3 PRA Objectives and Ground Rules

a. The objective of the risk assessment ***shall*** be well defined, and associated with it, the appropriate undesirable consequences of interest. The maximum allowable probability of occurrence for undesirable consequences ***shall*** be set by the program or project.

b. The program/project systems engineering and components engineering groups will respond to qualitative and quantitative implications of the PRA by addressing design areas where improvement is needed in order to reduce the risk below the maximum allowable value.

c. Ground rules for both scope and detail should be developed and reviewed by the PM and cognizant S&MA organization.

7.2.4 Application of PRA

a. Utilizing the PRA process, the program or project ***shall*** work with Safety and Mission Assurance (SMA) to identify weaknesses and vulnerabilities in a system that can adversely impact safety, performance, and mission success. The program/project engineers ***shall*** work with SMA to recommend controls (preventive and mitigating features and compensatory measures) needed to reduce and manage risks. Information on design that is required to update PRA models and analyses ***shall*** be provided by design and systems engineering.

7.2.5 Requirement for an Integrated Process

a. The PRA process and analytical activities ***shall*** be integrated with the design and development process, systems engineering, RM, safety, and SA. The SMA disciplines will provide information and data to PRA practitioners. (Examples are Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL), Hazards Analysis and Safety Data Packages, Fault Tree Analysis, Reliability Analysis Reports, and Software Fault Analysis.) The design and systems Engineers ***shall*** provide information, data, and a design and operational description to support the development of the PRA. The draft reports will be provided to SMA disciplines and to program/project engineers for review.

7.2.6 PRA Management

a. Each program/project that is required to perform a PRA ***shall*** track the progress of the PRA activity against major milestones. At major milestone reviews, progress toward achieving the risk reduction requirement (the maximum allowable probability of occurrence for a defined end-state, such as loss of crew, loss of mission, or loss of vehicle) ***shall*** be reviewed. Identification of areas for improvement will be provided.

7.2.7 PRA Plan

a. The PMs and the SR&QA managers ***shall*** ensure that the plan for conducting the PRA is prepared, is tailored in order to apply to the specific program or project, and addresses the requirements specified in the Space Assurance Requirements (SAR) document for PRA. The PRA effort for each program/project ***shall*** be governed by the PRA plan that is contained in the program/project's SMAP. If specific requirements do not apply to a program or project or will not be implemented for various reasons, the requirement area is documented in the SMAP as "not planned" and with a rationale.

Chapter 8. Quality Assurance Requirements

8.1 General Requirements

a. The program/project ***shall*** maintain an effective quality assurance (QA) program, which assures that quality requirements are met through control of design, operations, processes, procedures, testing, and inspection. See Chapter 10 for software product requirements. The QA program ***shall*** meet the intent of NPD 1280.1 and NPD 8730.5 and ***shall*** be implemented by GLPD 8730.5, GLPR 8730.5, and GLPR 8730.6.

b. The QA program ***shall***:

(1) Be designed and implemented in a manner that mitigates risks associated with noncompliance. Determination of risk considers the likelihood of noncompliance and the consequences associated with noncompliance, including the maturity, complexity, criticality, and value of work performed, as well as demonstrated experience with past quality system or program performance.

(2) Attain confidence levels for requirement compliance that are commensurate with the severity of consequences that would be incurred in the event of noncompliance.

(a) For circumstances where noncompliance cannot result in loss of life or loss of mission, statistically based sampling plans or 100 percent inspection ***shall*** be employed based on determination of risk.

(b) For circumstances where noncompliance can result in loss of life or loss of mission, Government Mandatory Inspection Points (GMIP) ***shall*** be performed to ensure 100 percent compliance with safety/mission critical attributes. Safety/mission critical attributes include hardware characteristics, manufacturing process requirements, operating conditions, and functional performance criteria that, if not met, can result in loss of life or loss of mission.

(3) Be reevaluated and adjusted based on changes to risk factors.

(4) Include prework assurance measures that provide increased confidence for meeting prescribed requirements (e.g., preaward surveys, qualified source selection, and training), concurrent assurance measures to ensure that work is being performed in accordance with requirements (e.g., process control and process witnessing), and post-work assurance measures to ensure that work was properly performed (e.g., inspections, tests, record review, and configuration control).

(5) Flow applicable QA requirements down to successive levels of the supply chain to ensure control of subtier suppliers and verification of safety/mission critical attributes at all levels of the supply chain.

(6) Continually be improved through advocacy, awareness training, teaming, sharing of QA tools, techniques and data, integration of QA processes to prevent duplication of effort, and dissemination/implementation of lessons learned and best practices.

(7) Ensure that customers and government authorities are quickly notified concerning noncompliant products or failure experiences potentially affecting product safety, reliability, or functionality. Customers and government authorities include contracting officers; Government

contract management agents; authorities responsible for assigning, managing, or overseeing work; and where noncompliant conditions might constitute evidence of possible fraud, malpractice, or other serious misconduct, the NASA Office of Inspector General.

(8) Provide for investigative and corrective actions upon discovery or notification of noncompliance.

c. Investigative actions ***shall*** identify the proximate and root cause(s) of noncompliance and the scope/population of noncompliant items.

d. Corrective actions ***shall*** include the correction, replacement, repair, or authorized disposition of noncompliant items/conditions, implementation of preventive measures to eliminate the causes of noncompliance, and validation that implemented preventive measures have effectively eliminated recurrence of the noncompliant condition (recurrence control).

(1) Ensure clear and mutual understanding of prescribed quality requirements among organizations responsible for contracting or assigning work, performing work, and assuring conformity of work.

(2) Be performed by persons that are competent on the basis of

e. Demonstrated knowledge, skills, and experience related to QA principles and practices, and related to the specific product, process, or attribute for which assurance is being provided.

f. Meeting formal certification or qualification requirements where prescribed in required/invoked documents or where deemed necessary to ensure personnel competency to perform specialized QA functions.

(1) Be performed by persons that are not assigned direct responsibility for ensuring that cost or schedule objectives are met.

(2) Be supported by records demonstrating compliance with technical/quality requirements. Records ***shall*** be legible, traceable to the applicable product, identifiable to the applicable requirement, and readily retrievable for requirement verification.

(3) Include the collection and analysis of quality data for the purpose of identifying and initiating resolution of problem areas (e.g., projects, products, processes, operations, and organizations), common deficiency causes, nonconformance trends, defect anomalies, and process variations.

g. Government QA organizations are to ensure that contractors implement quality system requirements and deliver conforming product in accordance with Federal Acquisition Regulation (FAR), the NASA FAR Supplement, and NPR 8735.2, Management of Government Safety and Mission Assurance Functions for NASA contracts.

h. Every program/project ***shall*** develop a QA plan. The QA plan is designed to be a technical planning guide for the technical performance and management of the quality assurance activities. The QA plan can be a standalone document, or part of the Safety and Mission Assurance Plan (SMAP).

8.2 Quality Assurance Organization

a. The program/project ***shall*** designate an individual who is responsible for directing and managing the QA program. The program/project ***shall*** make functional assignments to implement each element of the quality program. Personnel performing quality program functions

shall have sufficient, well-defined responsibilities and the organizational freedom to identify and assess problems, and to recommend, track, and review solutions. The effectiveness of quality program functions and the ability of assigned personnel to objectively assess, document, and report findings ***shall*** be maintained during all phases of the program/project and ***shall*** not be reduced by other considerations, such as the influence of engineering changes, rework, or rescheduling.

8.3 Configuration Management (CM) and Verification

a. All documents, drawings, and revisions, which define and verify the system, ***shall*** be kept under configuration control per *GLPR 7123.34* (*future document*). A CM plan ***shall*** be developed, which will specify responsibilities, and as a minimum, address the following:

(1) Identification of configuration items, which will be baselined and controlled, including specifications and procedures.

(2) Formation of a Configuration Control Board (CCB) to review baselined items, and to review changes to controlled items. The duties of the board, along with responsibilities, ***shall*** be based on the complexity of the design and be specified in the CM plan.

(3) The completion of an as-built list, which will document the final versions of the components contained in the flight system, along with a verification that all testing and changes have been properly completed in both documentation and the system.

(4) Records of all changes made to the system once the configuration items have been baselined.

b. The system configuration items ***shall*** be placed under configuration control and baselined at the earliest possible time. This will occur at the time an assembly is considered to be in a flight-like configuration. This may be at the engineering, functional, or proto-flight model stage, but in all cases, the system ***shall*** be baselined by critical design review (CDR).

c. The responsible program/project configuration control personnel ***shall*** assure that documents are kept current, and when changes are made, they are made promptly and include changes to all associated documentation and the system. The CM plan ***shall*** assure that only the latest drawings, including all changes, are used for the fabrication, assembly, testing, and inspection of all components.

d. Inspection records ***shall*** indicate the revision level with which the item has been fabricated, inspected, and/or tested. Evidence ***shall*** be provided specifying compliance with the as-built documentation as a basis for acceptance.

e. Please refer to Section 10.5 of this document for a discussion of software configuration management.

8.4 Identification and Traceability

a. A system identification and tracking procedure ***shall*** be established, which identifies each part by a unique part or type number, consistent with the CM system. The CM system ***shall*** be capable of retrieving the identification and serialization record at the subassembly level. Beginning at the subassembly level and continuing through the end system, the procedure ***shall*** be capable of tracing backwards to the originating subassembly and forward to the location of the subassembly at any given level of process, assembly, or test. Identification and serialization data lower than that for subassemblies ***shall*** be maintained in the manufacturing and processing

records, and ***shall*** contain part and material date code, lot number, and manufacturer information.

8.5 Procurement Requirements

a. All procurement ***shall*** include the appropriate QA requirements for the task. Where the complexity or criticality of the component is high, a process capability survey ***shall*** be performed at the manufacturing facility.

b. If inspections, tests, or processes need to be verified at the manufacturer/supplier's plant, the procurement document ***shall*** so indicate. Examples of when such inspections, tests, or verifications are needed include:

(1) When in-process or end-item controls have an impact on the performance or quality of the product, and the quality cannot be determined solely by receiving inspection or acceptance tests.

(2) When environment or test equipment needed to perform any verification is technically and economically feasible.

(3) History of the manufacturer/supplier shows risk.

(4) Qualification testing is to be performed by the manufacturer/supplier.

8.5.1 Government Source Inspection

a. All purchase orders ***shall*** include a statement which assures that the government has the right to inspect any or all of the work included in the purchase order.

8.5.2 Receiving Inspection

a. A receiving inspection system ***shall*** be developed and implemented which ensures purchased components comply with procurement documents. The receiving inspection system ***shall*** verify that:

(1) Documentation is reviewed to verify that components comply with purchase requirements.

(2) Inspections and/or tests are performed in accordance with written procedures for selected components to verify performance.

(3) Identification of acceptance or nonconformance status of components and records is maintained. All nonconforming items ***shall*** be segregated for disposition.

(4) Receiving inspection and test records are maintained.

(5) Protective measures for cleanliness, electrostatic discharge, handling, packaging, and shipping are implemented.

8.6 Control of Fabrication Activities

a. A fabrication and assembly flow process ***shall*** be developed and implemented that covers operations from start of fabrication to end item completion. Inspection and test points and all special processes to be used ***shall*** be included. Controls ***shall*** ensure that only conforming components are released and used during fabrication.

8.6.1 Fabrication and Inspection Requirements

a. Suitable fabrication and inspection requirements ***shall*** be used based on the complexity and expected environment of the program/project. All drawings ***shall*** meet the requirements of American Society of Mechanical Engineers Y14.5. Only released prints, approved in accordance with the configuration control plan, ***shall*** be used for the manufacture of the qualification and flight hardware.

8.6.1.1 Control of Assembly, Inspection, and Test Activities

a. The program/project ***shall*** plan and conduct an assembly, inspection, and test program, which controls fabrication, assembly, testing of flight systems, and demonstrates that drawing and specification requirements are met. The assembly, inspection, and test plans ***shall*** be approved prior to work being performed on flight articles. Inspections and performance tests ***shall*** be performed on components and subassemblies when they cannot be fully inspected or tested in the next level of assembly. Each inspection and test ***shall*** be traceable to the person performing the task. The program/project and/or developer's QA organization ***shall*** verify that all manufacturing documentation, processes, procedures, and specifications are available prior to the build.

8.6.1.2 Assembly, Inspection, and Test (AIT) Procedures

a. All work and inspections performed on flight hardware/software ***shall*** be conducted with approved procedures per the CM plan. Proper planning ***shall*** be done to ensure orderly and timely inspections are performed at all levels of assembly and tests.

b. The AIT procedures ***shall*** be written for all flight system operations. The degree of detail in the procedures ***shall*** commensurate with the complexity of the operation. Drawings may stand alone as assembly procedures as appropriate. Written assurances that these procedures were followed ***shall*** be provided in a logbook. Any deviations from these procedures must be properly approved and recorded per the CM plan. Each system operation ***shall*** have a responsible individual for its accomplishment. The responsible individual's name ***shall*** be recorded in the logbook.

c. Procedures ***shall*** include, as applicable, the revision level of the document, the nomenclature of the article, instructions for qualified personnel to perform the work, characteristics to be inspected or tested, accept/reject criteria, and special considerations regarding handling, measuring, testing, equipment, standards, safety, and environment. The program/project and or developer's QA organization ***shall*** verify that proper inspection and testing criteria are included in the procedures during the QA review of processes, procedures, and specifications. Prior to any testing or inspection QA ***shall*** assure that all applicable procedures are available, test/inspection equipment is calibrated and properly configured, and the facility is properly configured. Procedures ***shall*** require the recording of equipment identification and calibration due dates for all calibrated instruments used. During testing, the QA assures the testing/inspection is performed with the approved procedures. After testing/inspection, the QA assures the results and data are complete and traceable to the appropriate test article. The logbooks of this activity must be kept in sufficient detail to verify and evaluate the status of all articles and materials tested/inspected.

8.6.2 Training for Personnel

a. The program/project ***shall*** establish and maintain documented procedures for identifying training needs and provide for the training of all personnel performing activities affecting quality. Personnel performing specific assigned tasks ***shall*** be qualified on the basis of appropriate education, training and/or experience, as required. The PM ***shall*** specify in the program/project plan the training needs for the program/project. Appropriate records of training ***shall*** be maintained (see Section 8.17).

8.6.3 Evaluation and Control of Process Specifications and Procedures

a. All specifications and procedures for processes ***shall*** be evaluated to ensure compliance to program/project requirements. Special processes, with which the quality cannot be ensured by inspection alone, ***shall*** be given special attention as to the controls and methods of verifying the adequacy of the process. The developer's QA organization ***shall*** assure all processes are adequate for the stated purpose. The following list of special process and inspection documents are requirements for all NASA GRC flight hardware: NASA-STD-8739.1, NASA-STD-8739.2, NASA-STD-8739.3, NASA-STD-8739.4, NASA-STD-8739.5, IPC-2221, and IPC-2222. Other requirements ***shall*** be imposed by the program/project as deemed necessary.

8.6.4 Bonded Storage

a. The program/project ***shall*** maintain a controlled bonded storage area, which is capable of storing flight material, parts, and assemblies. The level and type of environmental control ***shall*** be defined based on the specifics of the flight material, parts, and assemblies being stored. The environmental control ***shall*** minimally protect the flight items from excessive temperatures and humidity, and from contamination. Electrostatic discharge (ESD) control ***shall*** be implemented for ESD sensitive parts as defined in Section 8.8.

b. The area ***shall*** have controlled access applicable to the type of system being held, and ***shall*** have a documentation system adequate to identify and track the flow of parts in and out of bonded storage. Bonded storage ***shall*** be capable of segregating materials, assemblies, qualified components, accepted systems, limited-life items, and nonconforming components. Traceability by part number, manufacturer, serial numbers, and lot date code ***shall*** be maintained for parts and components in controlled storage.

8.6.5 Records of Inspections and Tests

a. Records ***shall*** be maintained of all inspections and tests as evidence that all operations have been performed, objectives have been met, and the end-item is fully verified. Logbooks ***shall*** be kept for each component, subassembly, and assembly, based on their complexity. As the product is integrated, the next higher-level assembly documentation ***shall*** reference all integrated subassemblies or subsystems by positive configuration identification. The logbooks ***shall*** document all actions taken on the component, and ***shall*** provide for easily accessible total operating time of the component under control.

8.7 Contamination Control

a. The program/project ***shall*** assure compliance to the contamination requirements during all phases of the program or project.

b. Contaminants include all materials of molecular or of particulate nature whose presence degrades system performance. The source of the contaminant materials may be the system itself, the test facilities, and the environments to which the system is exposed.

8.7.1 Contamination Control Plan

a. The program/project ***shall*** prepare and implement a contamination control plan (CCP) that describes methods for controlling contaminants and verifying that they have been prevented or abated such that the hardware will meet performance requirements. The CCP ***shall*** be submitted for approval by the GRC project management and the GRC program/project assurance manager prior to work being performed on flight hardware. Analyses, procedures, standards, processes, and specifications referenced in the CCP ***shall*** be available for review at the developer's facility.

b. The CCP ***shall*** define contamination allowances for performance degradation of contamination-sensitive systems such that, even in the degraded state, the system will meet its mission objectives. Allowable contamination levels are either those necessary to ensure that the system will meet its performance requirements or those necessary to meet mission contamination control considerations, whichever is more stringent. The allowance and the rationale for allowable levels ***shall*** be described in the CCP. These levels ***shall*** serve as a basis for the measurements to be taken to control contamination. The contamination allowable ***shall*** be assessed in a timely fashion such that results can be used to assess the adequacy of, and if necessary, to modify the design of the system.

c. The CCP ***shall*** describe methods for controlling contamination and for ensuring that the contamination allowance is not exceeded. It ***shall*** identify the controls, process, inspections, productions, test, assembly, methodology, analyses, and documentation necessary to measuring and maintaining the levels of cleanliness required during the various phases of the system's lifetime.

d. The CCP ***shall*** identify controls to be exercised in preparing test facilities, such as the thermal-vacuum chamber and fixtures. It ***shall*** also identify the operational procedures that will be followed to minimize the contamination hazard during various test phases, such as from pump down through return to ambient conditions. Appropriate pretest measurements, monitoring methods to be used during the tests, and post-test measurement ***shall*** be identified.

e. Bake outs of hardware ***shall*** be required based on the materials evaluation and use environment. When required, the parameters of such bake outs (e.g., temperature, duration, and pressure) must be individualized depending on materials used, the fabrication environment, and the established contamination allowance.

f. The contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, and bagging (e.g., antistatic film materials), ***shall*** be considered. Clean room standards and personnel training ***shall*** also be included in the processes.

8.8 Electrostatic Discharge Prevention

a. The developer ***shall*** plan, implement, and maintain a program to prevent ESD damage to any susceptible parts or components in accordance with ANSI/ESD S20.20. Personnel who handle ESD sensitive parts or components ***shall*** be trained in ESD prevention methods.

8.9 Nonconformance and Problem Reporting and Control

a. The program/project ***shall*** report failures and nonconformances through a documented problem reporting and corrective action (PRACA) system. In-house programs/projects ***shall*** handle PRACA through the GRC Corrective and Preventive Action Reporting System (CPARS) (Ref. GLPR 1270.1). An outside contractor may maintain its own PRACA system with approval of the PM and Chief Safety and Mission Assurance Officer (CSO). The program/project ***shall*** implement the PRACA system during the development phase within the program/project team. The PRACA review board and review process ***shall*** be initiated prior to subsystem testing and system level assembly for the prototype and flight systems prior to system-level testing. The PRACA system ***shall*** include documentation of problem, traceability of material or part, disposition of problem, root cause corrective action, segregation of discrepant material, verification of corrective action, and trending to help prevent similar discrepancies. The SMAP ***shall*** describe the problem review process including any review boards and the problem report tracking and distribution process. The NASA ***shall*** be informed of any reportable problem within 48 hours of occurrence.

b. A reportable problem is any nonconformance which is, or is suspected of being, a failure, an unsatisfactory condition, an unexplained anomaly, or an overstress occurring during or subsequent to production acceptance testing or qualification testing (i.e., after manufacturing or development).

c. The problem report should include as a minimum: (1) description of problem, (2) analysis of root cause of problem, (3) description of corrective action, and (4) corrective action follow-up.

8.9.1 Review Boards

a. A review board ***shall*** be operated with the responsibility of reviewing all problem reports. The board ***shall*** include the following:

(1) Quality or reliability representative (chairman)

(2) Engineering representative

(3) PM or his/her representative (necessary for failure board only)

(4) Government representative, if other members are contractor personnel

b. The board ***shall*** have the authority and responsibility to:

(1) Determine the disposition of the submitted problem.

(2) Approve all standard repair procedures.

(3) Ensure that remedial and preventative actions are properly addressed.

(4) Ensure that excessive repairs do not compromise the component’s reliability and quality.

8.9.2 Waivers and Deviations

a. The acceptance of any nonconformance affecting flight acceptance, safety, or mission success ***shall*** require an approved waiver or deviation. The SMAP ***shall*** describe the process for submission, review, and disposition of a request for waiver or deviation. The process defined in *GLPR 7120.14 (under development)*, GRC Deviation/Waiver Process, ***shall*** be used to document and approve any deviations or waivers.

8.10 Alert Information

a. The program/project ***shall*** review NASA Parts Advisories and Government-Industry Data Exchange Program (GIDEP) Failure Experience reports according to the requirements of NPR 8735.1 and respond to Program and Project Assurance Division and program/project review teams as to the applicability to program/project systems, location of affected system, criticality identification from the Failure Modes and Effects Analysis and Critical Items List and disposition for design reviews. The GIDEP failure experience reports include GIDEP ALERTs, SAFE-ALERTs, problem advisories, and Agency action notices.

b. The program/project ***shall*** report discrepant parts and/or components that are within the scope of the GIDEP Failure Experience system or NASA Parts Advisory system to the GRC GIDEP Coordinator (Program and Project Assurance Division), who ***shall*** prepare and submit the failure experience report to GIDEP or issue the NASA Parts Advisory per NPR 8735.1. A contractor may use its own GIDEP representative to prepare and submit the GIDEP Failure Experience report, but ***shall*** inform the GRC PM and CSO of the problem and provide them with an advance copy of the report.

c. The list below shows Web sites where more information can be found:

(1) GIDEP Home Page

(2) The NASA Parts Advisories are available in the NASA Advisory Forum (requires username and password)

(3) The GIDEP database for alert searches (requires username and password)

d. Contact the CSO for software to conduct electromechanical parts alert searches.

8.11 Inspection and Test of Stored Limited-Life Hardware

a. A test plan ***shall*** be developed, which assures that limited-life items stored or stocked have not been degraded or damaged during storage. The plan ***shall*** address proper handling, including environmental conditions, to mitigate damage or prolong life, and testing to assure the stored items meet required specifications. Limited-life items not meeting the requirements set forth in the plan ***shall*** be considered nonconforming, and handled in accordance with Section 8.9. Limited-life items ***shall*** be identified on a list and a log of their remaining life maintained.

8.12 Metrology

a. The program/project ***shall*** establish and implement a documented metrology system in accordance with NPD 8730.1. Only properly calibrated instruments and tools ***shall*** be used to assemble, test, inspect, and verify flight hardware. Individual records of measurement standards and equipment ***shall*** be maintained. Records include identification of standard use, identification of equipment calibrated, identification of calibration procedure used, calibration time interval to next calibration, results of calibration, and individuals performing the calibration.

8.13Handling, Preservation, Marking, Packaging, Packing, and Transportation

a. The program/project ***shall*** develop and implement procedures for handling, preservation, marking, packaging, packing, and transportation to properly protect and identify all flight systems and ground support equipment during buildup, handling, storage, testing, shipping, and

turn-over at integration. The program/project's QA organization ***shall*** verify that the articles and materials have been prepared and packaged in accordance with applicable procedures and requirements and have been properly identified and marked. Also all accompanying documents ***shall*** have been properly identified as to inspection status with the appropriate inspection stamps.

8.13.1 Control of Government Property by Contractors

a. When supplied in accordance with the provisions of the contract, government property ***shall*** be controlled and accounted for by the contractor. The contractor ***shall*** be responsible for, at minimum:

(1) Upon receipt, examine components to detect damage that may have occurred in transit.

(2) Inspect for quantity, completeness of shipment, and proper shipping documents.

(3) Provisions for protection, maintenance, calibration, periodic inspection, and controls necessary to prevent damage or deterioration during handling, storage, installation, or shipment.

b. Any property that is found damaged, malfunctioning, or otherwise unsuitable for use ***shall*** be processed in accordance with government procedures and Section 8.9. The property ***shall*** not be disposed of, repaired, reworked, replaced, or in any way modified unless such actions are authorized by or prior approval of GRC's PM and the contracting officer.

8.14 Configuration Verification

a. The program/project's CM System ***shall*** be capable of assuring that as-built hardware conforms to the design documentation. The program/project's QA organization will provide assessment of the CM system during construction of the engineering and flight systems. Formal verification and sign off that flight as-built systems conform to as-designed documentation ***shall*** be the responsibility of the program/project, unless otherwise stated in the SMAP.

b. Prior to GRC developed hardware being shipped from GRC or prior to the hardware turnover to the project integrator or customer, a preship review (PSR) ***shall*** be held, reference *GLPR 7123.21 (under development)*, Product Transition. As an outcome of a successful PSR, or at the satisfactory completion of all open work assigned as a result of the PSR, the PM ***shall*** initiate the GRC Certificate of Flight Readiness (CoFR) signature cycle. The GRC CoFR signature page and GRC CoFR formats are found in Appendix 0. Copies of the signed form should be kept in permanent program/project records according to the program/project's records management system.

8.15 Acceptance of Flight System

a. Prior to the preship review the program/project ***shall*** assure that all deliverable end-items including the acceptance data package are in accordance with program/project requirements. The acceptance data package ***shall*** be submitted for GRC approval and includes as a minimum the following:

(1) As-built configuration list in accordance with Section 8.3

(2) List of as-built parts used in accordance with Chapter 5

(3) List of materials and processes used in accordance with Chapter 6

(4) Log books, including total operating and repair times, and cycle records

(5) Status of all verification items with a list of open items and rationale for the items being open

(6) Listing, status, and remaining life of limited-life items

(7) Results of Flight Acceptance Tests

(8) Listing and status of all nonconformance, failure, or problem reports

(9) Listing of waivers and deviations affecting flight acceptance, safety, and mission success

(10) Cleanliness certification

(11) Certification of flight software acceptance in accordance with Chapter 10

8.16 Quality Program Audits

a. The QA ***shall*** conduct audits of task performance, procedures, and operations, which implement the quality program. Assessments ***shall*** be conducted periodically, as appropriate, with program maturity and ***shall*** be performed by personnel not having specific line responsibilities in those areas. Each audit ***shall*** include an examination of operations and documentation, evaluation of actual operations as compared with each established requirement, documentation of discrepancies and deficiencies, and recommendations for corrective action, as appropriate. A corrective action plan, which addresses measures to be taken to correct the discrepancies/deficiencies, ***shall*** include reviews to ensure that measures required by the corrective action plan are being implemented properly.

b. The results of audits ***shall*** be documented in a report to management. Management action ***shall*** be taken to ensure correction of the reported deficiencies. Follow-up reviews ***shall*** be made to ensure that required corrections have been implemented. Records of the audits ***shall*** be available for review by the program/project or its delegated representative.

8.17 Control of Quality Records

a. The program/project ***shall*** establish and maintain documented procedures for identification, collection, indexing, access, filing, storage, maintenance, and disposition of quality records. The quality records ***shall*** be maintained to demonstrate conformance to specified requirements and the effective operation of the quality system. Pertinent quality records from the subcontractor ***shall*** be an element of these data.

Chapter 9. Continuous Risk Management

9.1 Risk

a. According to NASA NPR 8000.4, risk is characterized by the combination of the probability that a program or project will experience an undesired event and the consequences or severity of the undesired event, where it is to occur. A risk is not a problem. The problem has already happened and should be tracked in the appropriate problem reporting database.

9.2 Introduction

a. Risk Management (RM) is a set of activities aimed at achieving success by proactively risk-informing the selection of decision alternatives and then managing the implementation risks associated with the selected alternative. Per NPR 8000.4, the RM is defined in terms of risk informed decision making (RIDM) and continuous risk management (CRM). The document addresses the application of these processes to the safety, technical, cost, and schedule mission execution domains throughout the life cycle of programs and projects, including acquisition. In addition, institutional risks and the coordination of RM activities across organizational units are addressed.

b. The purpose of integrating RIDM and CRM into a coherent framework is to foster proactive RM to better inform decision making through better use of risk information, and then to more effectively manage implementation risks using the CRM process, which is focused on the baseline performance requirements emerging from the RIDM process. Within a RIDM process, decisions are made with regard to outcomes of the decision alternatives, taking into account applicable risks and uncertainties; then, as part of the implementation process, CRM is used to manage those risks in order to achieve the performance levels that drove the selection of a particular alternative. Proactive RM applies to programs, projects, and institutional or mission support offices.

9.2.1 Risk Informed Decision Making (RIDM)

a. The RIDM incorporates risk analysis in the design and formulation of the program baseline. The process of RIDM considers diverse performance measures, which characterize the performance a system, process, or activity in fulfilling its intended objectives (performance measures may relate to system, mission, safety, or cost performances). The RIDM advocates: top-down and integrated modeling of performance measures, consideration of uncertainties in risk characterization and acceptance, and deliberation to address issues that have not been captured by the formal analysis.

b. The RIDM manages threats to satisfaction of baseline performance requirements by assessing risk associated with implementation of the selected alternative, assisting in setting resource priorities (including prioritization of work to resolve uncertainties if warranted), plan/track/control risk during the implementation of the selected alternative, and iterate with previous steps in light of new information.

9.2.2 Continuous Risk Management

a. The CRM is an organized, systematic decision-making process that efficiently and effectively identifies, analyzes, plans (for the handling of risks), tracks, controls, communicates, and

documents risk to increase the likelihood of achieving program/project goals. The RM is a continuous, iterative process to manage risk and should be an integral part of normal program/project management and engineering processes. The CRM provides a disciplined environment for proactive decision making to:

(1) Assess continually what could go wrong (risks)

(2) Determine which risks are important to deal with

(3) Implement strategies to deal with those risks

(4) Assure and measure the effectiveness of the implemented strategies (or mitigations)

9.2.3 RIDM and CRM

a. Both CRM and RIDM are applied within a graded approach. The resources and depth of analysis need to commensurate with the stakes and the complexity of the decision situations being addressed. For example, the level of rigor needed in risk analysis to demonstrate satisfaction of safety-related performance requirements depends on specific characteristics of the situation: how stringent the requirements are, how complex and diverse the hazards are, and how large the uncertainties are compared to operating margin, among other things. Both RIDM and CRM are formulated to allow for this.

9.2.4 Institutional Risks

a. The management of institutional risks affecting multiple programs/projects is carried out within Center support hierarchy and coordinated with the program/project offices as needed. Since the program/project offices are affected by institutional risks without being in a position to manage them proactively, in the event that institutional risks threaten accomplishment of program/project office performance requirements, the program/project office need either to manage those risks with their own resources or elevate them to the next level within the program/project hierarchy.

9.3 General Requirements

a. The NASA directive NPR 7120.5, “NASA Program and Project Management Processes and Requirements,” provides the basic RM requirements that are applicable to all programs and projects. The Center’s GLPR 8000.1 implements the RM provisions of the NPR 7120.5 while *GLPR 7123.33 (under development)* establishes the framework for conducting RM across programmatic, financial, and institutional activities. Both these documents require that each NASA program and project will develop and operate, plan, and execute using RM decision processes. The program or project is required to implement a plan to mitigate, close, or accept each risk in the most resource-effective manner, based on its impact on the program or project mission’s objectives.

b. Each program/project that provides aerospace products and capabilities (i.e., space, aeronautics, flight and ground systems, technology, research and analysis, and operations (test and computational), and any component facilities and institutional operations at GRC ***shall*** address and implement CRM. The CRM is not required but may be used for activities such as nonflight infrastructure, Construction of Facilities, and Small Business Innovation Research (SBIR) projects.).

c. Each program/project ***shall*** develop a RM plan in accordance with the provisions of NPR 7120.5 and NPR 8000.4. The RM plan ***shall*** be developed during the formulation phase and executed/maintained throughout the life cycle of the program/project. The RM plan can be a standalone document or as part of the program/project plan and ***shall*** document how risks will be managed: the processes, activities, responsibilities, milestones, and resources associated with RM.

d. The RM for the various programs/projects at GRC involves two steps: Initial RM training for the program/project team, and then implementation. The methodology of this training and implementation may be unique and tailored for each program/project at the discretion of the Assurance and Risk Management Branch.

9.4 Initial Risk Management Training

a. The Program and Project Assurance Division offers three training courses, which serve to impart a methodology that satisfies the NASA requirement for implementing RM. A program/project should use RM training to build teamwork. The RM training involves personnel at all levels of the program/project, focuses their attention on a shared product vision, and provides a mechanism for achieving the program/project's mission objectives.

9.5 Implementation

a. The program/project ***shall*** do RM as part of their program management. Implementation of CRM is required by NPR 7120.5 and involves six fundamental steps, as discussed below. Each program/project ***shall*** define and implement a means of accomplishing each of the six steps. The Assurance and Risk Management Branch is chartered to provide a wide range of technical assistance in the CRM process, from consultation/facilitation to extensive training and implementation activities.

9.5.1 Identify Risks

a. Identification of risks by examining program/project data and constraints is the process of transforming uncertainties and issues about a program/project into distinct (tangible) risks that can be described and measured. The goal of risk identification activities is to search for and locate risks before they become major problems. Risk identification is a continuous process, because new risks can be identified throughout the program/project's life cycle. Some of the methods that can be used to identify risks are the expert interviews, brainstorming, searching lessons learned, failure modes and effects, analysis, fault tree analysis, systematic analysis of work breakdown structure levels, and comparison of program/project goals with plans. The key program/project areas to assess are requirements, technology used, management, engineering, manufacturing, supportability (logistics and maintainability), operations, safety, and programmatic aspects. Sources of information on risks include metrics, historical data, resources used, suppliers used, plans, proposed changes, test results, and program/project personnel.

b. Identifying risks involves two activities: capturing a statement of risk and capturing the context. Capturing a statement of a risk involves considering and recording condition that is causing concern for a potential loss to the program/project, followed by a brief description of the potential consequences of this condition. The format of a risk statement is: *Given the* [**condition that is causing anxiety**]; *there is a possibility that* {**consequence**} *will occur.*

c. The second activity involves documenting additional information regarding the circumstances, events, and interrelationships within the program/project that may affect the risk. The additional information about the risk ensures that the original intent of the risk can be easily understood by other personnel, particularly after time has passed.

9.5.2 Analyzing Risks

a. The primary function of analyzing risks is examining the risks in detail to determine the extent of the risks, how they relate to each other, and which ones are the most important. During analysis, the risk data is converted into decision-making information. The risks are evaluated by assessing the likelihood of the risk events occurring, as well as the consequences of the risk occurrences to determine the relative importance. The consequences of risk occurrence include cost, schedule, performance, and safety impacts. The risk attributes (likelihood and consequences: cost, schedule, performance, and safety) are defined by a governing RM plan or by the program/project prior to identifying risks.

b. The risks are then classified or grouped based on shared characteristics to help the program/project understand the risks. The duplicate risks are identified and some risks can be grouped into sets to help build more cost-effective mitigation plans. Finally, risks are prioritized to determine which risks should be dealt with first when allocating resources. Prioritization of risks should be based on the criteria for what is most important to the program/project.

9.5.3 Planning

a. After the risk is identified and analyzed, it is necessary to determine what to do about the risk. The risk planning involves translating risk information into decisions and mitigating actions (both present and future), and implement those actions. The risks are planned by those who have the knowledge, expertise, background, and resources to effectively deal with the risks. Planning answers the questions:

(1) Is it my risk or responsibility?

(2) What approach can I take with this risk?

(3) How much and what should I do with this risk?

b. Risks are reviewed to make sure that they are understood and clearly documented. Responsibility for the risk is then assigned. An approach for dealing with the risk is determined by the responsible person or team. Additional research may be needed, the risk could be accepted as is, could be watched, or could be mitigated. If the risk is mitigated, a mitigation plan is developed and ultimately implemented to minimize the risk and impacts while maximizing opportunity and value.

c. There are many constraints (e.g., program/project schedule limits, hard milestones, available personnel, hardware restrictions, total cost of risk impact, facility capacity and availability, RM budget) that can affect risk planning. These will vary with each program/project and situation. It is important to identify these and periodically check to make sure the circumstances have not changed. Never take constraints for granted.

d. All risks cannot be planned simultaneously. The risks are planned in the order of importance, which depends on the goals and constraints of the program/project, managers, and individuals. However, priorities will change. When deciding on what approach to take, consider what is most

important to the program/project, which milestones are fixed or flexible, what resources are available, and if the risk fits into the overall program/project concerns.

e. Development of mitigation plans, accepting the risk, or recommending the transfer of the risk to a management authority (because it is out of the program/project's control to mitigate), are all actions to consider under the planning process. The development of mitigation plans may involve a trade study of various plans to find the best mitigation plan. The development of mitigation plans may involve contingency planning, wherein a mitigation plan is triggered in the future by some set of metric downturns in a tracked risk. The mitigation plan ***shall*** be developed to reduce, not necessarily eliminate, the likelihood of occurrence and/or the severity of the consequences. It may involve redesign, development of new prototypes, modification of the engineering requirements, augmentation of test, inspection, and analysis or finally renegotiation of the driving program/project requirements.

9.5.4 Risk Tracking

a. Tracking is a process in which risk data are acquired, compiled, and reported by the person responsible for tracking watched and mitigated risks. The data are collected and the results are compiled and presented in reports that are easily understood to the person/group who receives the status report. The status reports generated during tracking are used by program/project management during the control function of the paradigm to make decisions about managing risks.

b. Risks that are judged to have sufficiently severe consequences and high likelihood of occurrence ***shall*** be tracked and reevaluated periodically. (The actual time period between reviews is determined by the program/project, and should be generally stated in their RM Plan. It can also be tailored depending on individual risk severity.) Those risks, which have an active mitigation plan, ***shall*** be tracked and monitored to verify the mitigation is reducing the risks as planned. Those risks, which need communication to higher levels and boards, ***shall*** be actively communicated to the appropriate level (as defined in program/project documentation) in a timely manner. Any recommendations from these higher levels ***shall*** be carefully monitored to assure both the risk was properly understood and the suggested risk mitigation indicated was appropriate and doable with the resources given.

c. During tracking, the risk is monitored with indicators and triggers to determine if the mitigation plan is being followed and the risk severity is being reduced. Indicators provide insight into a process or improvement activity while triggers are thresholds for indicators that specify when an action such as implementing a contingency plan, may need to be taken. Triggers provide early warning of an impending critical event and that immediate action for a risk should be taken.

9.5.5 Risk Control

a. Control is the process of making informed, timely, and effective decisions regarding risks and their mitigation plans. Decisions are made by the project manager or the person who has accountability for the risk, based on current information from risk tracking as well as experience and are required to respond to changing conditions. Effective control includes execution of the planning phase, monitoring mitigation plan execution and effectiveness, assessment of risk changes and trends, determining appropriate responses, and communicating all the above

information. Risk tracking and control should be integrated with standard program/project management practices.

9.5.6 Communication and Documentation

a. At the core of the risk paradigm is open communication and documentation, which should be present in all other functions. Successful RM communication raises the level of understanding of relevant issues or actions within a program/project. The purpose of communication and documentation is for program/project personnel to understand the program/project's risks and mitigation alternatives, to understand the risk data, and to make informed choices within the constraints of the program/project.

b. Communication and documentation provide information and feedback to the program on risk activities, risk status, and potential new risks, and ensures the documentation and visibility of risk information for better management.

9.5.6.1 Risk Database

a. There is no requirement for where the risks should be maintained. However, for configuration management and for promoting teamwork, the risks should be located in a database where all have access. The Program and Project Assurance Division has developed a tool for local programs/projects and programs called Risk Management Implementation Tool (RMIT).

b. The RMIT is a Web-based tool that was designed to implement the NASA CRM process. This tool allows a program/project to identify, analyze, plan, track, control, document, and communicate risks in an environment tailored to their program/project requirements. Programs/projects can utilize RMIT as a basis for decisions on how to mitigate cost, schedule, technical, environmental, security, and safety risks. To ensure RM begins early in the life cycle, the programs/projects can begin using RMIT during the formulation phase to identify initial risks and develop a RM Plan, and then continue managing risks throughout the program's/project's life cycle.

c. The RMIT is centrally located for distributed program/project members to use, allows the risk owner to classify or group a risk with other risks, captures lessons learned, and is compliant with Section 508 requirements of the Rehabilitation Act. The RMIT features a flexible reporting format such as 5 X 5 Risk Matrix & Focus Chart, Waterfall Chart, Milestone Readiness, Top "N" Risks, Subsystems Affected, Days in System, Last Modified, Risk Classification, and Risks Summary Chart where project risks are listed along with their status.

9.5.6.2 Risk Reporting

a. The NASA has established a standard risk reporting format to communicate risks upward to the next management level and outward to other NASA Centers or NASA enterprises. The standard NASA risk report is a 5x5 risk matrix along with a top risk list that identifies primary risks per NPR 7120.5 and NPR 8000.4, as well as criticality and trending of the risk attributes. A Risk Focus Chart with detailed information about each risk is also required. Focus charts include risk identification number, risk title, risk statement, risk criticality, risk ranking, approach, current plan, the status of the plan, and the next milestone/action. As a minimum, all primary risks (red on the risk matrix) ***shall*** be reported in the format described above.

Chapter 10. Software Assurance

10.1 General Requirements

a. A software assurance (SA) program ***shall*** be established and maintained in accordance with NASA-STD-8739.8-Software Assurance Standard. The requirements of NASA-STD-8739.8 ***shall*** be implemented through GLPR 8739.1 for SA on the entire program/project life cycle. A software safety litmus test ***shall*** be performed and documented in accordance with GLPR 8739.1, Appendix G. A SA level of efforts ***shall*** be assessed by using Appendix E and F in GLPR 8739.1, and documented in accordance with GLPR 8739.1, Appendix H (Software Assurance Classification Report).

b. Every program/project ***shall*** develop a SA plan. The SA plan is designed to be a technical planning guide for the technical performance and management of the SA activities. The SA plan can be a standalone document, or part of the Safety and Mission Assurance Plan (SMAP).

10.1.1 Roles and Responsibilities

a. Successful implementation of the required SA processes and activities ***shall*** be the joined responsibility of the GRC program/project manager and PM, program/project software engineer(s), program/project SA manager, and the independent SA manager from the NASA GRC Safety and Mission Assurance Directorate (SMAD) assigned to the program/project. Details of these responsibilities can be found in GLPR 8739.1, Chapter 2. These responsibilities ***shall*** be documented in the SMAP.

10.1. 2 Scope of Software Assurance Activities

a. The scope of SA activities ***shall*** be in accordance with the software classification assessed per NPR 7150.2, GLPR 7150.1, and the assurance level of effort per GLPR 8739.1, Section P.2. Applicability ***shall*** be followed to determine the applicable SA scope.

10.2 Software Safety

a. A software safety litmus test ***shall*** be performed and documented per GLPR 8739.1, Appendix G. If the software is determined to be safety critical, then software safety activities ***shall*** be implemented, which maximizes the extent to which the developed software and electronic hardware perform their intended functions in a safe manner. Any software commands that could cause hazardous operations to occur ***shall*** be identified and documented.

b. A preliminary hazard analysis performed by the system safety engineer(s) assigned to the program/project ***shall*** include software safety and any potential software hazards ***shall*** be identified. A software safety requirements analysis ***shall*** be performed and documented in accordance to section 6 of NASA Software Safety Standard NASA-STD-8719.13. Measures ***shall*** be taken to provide for their elimination or control. The software safety activities performed in this area ***shall*** adhere to the requirements of NASA Software Safety Standard, NASA-STD-8719.13.

10.3 Software Reliability

a. Software reliability methods and activities ***shall*** be implemented, which assures that the developed software performs its required functions and meets its performance and fault tolerance requirements. The software fault tolerance requirements ***shall*** be identified through the use of software failure modes and effects analysis, software fault tree analysis, software errors trending, or other proven software reliability analysis and tools. The software reliability activities ***shall*** assure that the developed software ***shall*** not contribute to a total system failure as a result of external errors, an application, a process failing in a multitasking environment, or other conditions.

10.4 Software Configuration Management

a. A software configuration management process ***shall*** be implemented to manage requirements, design, code, data, and documentation, and to track and report on the status of changes to them. This process ***shall*** meet the requirements in GLPR 8040.1-Configuration Management (CM) & Data Management (DM), and ***shall*** be documented in a Software Configuration Management Plan (SCMP).

10.5 Software Nonconformance Reporting and Corrective Action

a. A process ***shall*** be established and maintained for the reporting, analysis, and correction of nonconformances, problems discovered in the software, and related documentation at the start of formal software testing. Formal software testing is defined as testing with baselined test procedures at the Computer Software Configuration Item (CSCI) Level. This process ***shall*** be continued until the software is retired from use.

b. This process ***shall*** meet the requirements in GLPR 1270.1-Corrective and Preventive Action. This process can be a component of the software CM function to the extent that change control is affected, and that reported nonconformances and change requests are identified and processed. A reporting process ***shall*** be established and maintained that shows the status and criticality of all nonconformances.

10.6 Software Verification and Validation

a. Verification and validation (V&V) processes ***shall*** be planned and implemented to demonstrate that the developed software meets system requirements and correctly provides the necessary functionality. The V&V processes ***shall*** include, but are not limited to, software reviews, walkthroughs or inspections, software testing, audits of the software development processes/products, final software acceptance, system testing, and mission sequence test.

10.6.1 Software Review

a. Various software reviews ***shall*** be conducted throughout the software development life cycle as defined in the program/project plan. Entrance and exit criteria for the software reviews ***shall*** be consistent with GLPR 7123.35, and contained in the specific software review plan. The program/project may elect to hold these reviews with formal presentations or may conduct them in a less-formal manner.

10.6.2 Software Inspections

a. Software formal inspections, peer reviews, and walkthrough of software development artifacts ***shall*** be conducted, as agreed to, in a program/project plan. Results of these activities ***shall*** be documented in the software development folder (SDF).

10.6.3 Software System Testing

a. All software system tests ***shall*** be performed in accordance with the established program/project plans and procedures. Any errors, defects, anomalies, or problems discovered during the test ***shall*** be documented by the program/project in the established Problem Reporting and Corrective Action (PRACA) system. The NASA-STD-8719.13 (Software Safety Standard), Section 6.4, ***shall*** be followed for testing safety-critical software.

10.6.4 Software Audits

a. An audit process ***shall*** be implemented for performing audits on the entire software development processes and products in accordance with program/project plans. This audit process ***shall*** be documented in the SA plan or the overall SMAP. At a minimum, a Physical Configuration Audit (PCA) and a Functional Configuration Audit (FCA) ***shall*** be performed during acceptance phase and prior to the software release. Additional information for FCA and PCA can be found in GLPR 8739.1, Appendix A.

b. Software audit process ***shall*** include the following audits:

Audits	Description	Responsibility Party	
		Provider SA	**Acquirer SA**
Functional Audit	This audit is held prior to the software delivery to verify that all requirements specified in the Software Requirements Document have been met.	Perform the audit and produce the audit report	Assure that the audit process comforms to established standards and procedures. Review audit report for completeness.
Physical Audit	This audit is held to verify internal consistency of the software and its documentation, and their readiness for release.	Perform the audit and produce the audit report	Assure that the audit process comforms to established standards and procedures. Review audit report for completeness.
In-process audits	In-process audits of samples of the design are held to verify the consistency of the design, including: a) Code versus design documentation b) Interface specifications c) Design implementation versus functional requirements d) Functional requirement versus test descriptions	Perform the audit and produce the audit report	Assure that the audit process comforms to established standards and procedures. Review audit report for completeness.

10.6.5 Software Acceptance

a. Prior to release of a given system (or acceptance by GRC of a contracted system), the GRC SA manager ***shall*** assure that software deliverable end-items associated with the Acceptance Data Package (ADP) are satisfactory. The ADP ***shall*** be signed off by the lead software engineer, the GRC SA manager, and the GRC PM.

Appendix A. Definitions

A.1 Acceptance Tests. The process that demonstrates that hardware is acceptable for flight. It also serves as a quality control screen to detect deficiencies, and normally to provide the basis for delivery of an item under terms of a contract (see Qualification Tests).

A.2 Assembly. A functional subdivision of a component, consisting of parts or subassemblies that perform functions necessary for the operation of the component as a whole. Examples are a power amplifier and gyroscope.

A.3 Audit. A review of a process to verify that it complies with the requirements.

A.4 Availability. The probability that a system will be operational at a given time. Availability consists of a transient contribution, which is initially high and decays away with time, and a steady-state component. Steady-state operational availability is the steady-state availability given the design reliability, maintainability, and logistics support capability; and is used to optimize levels of reliability, maintainability, and sparing support.

A.5 Catastrophic Hazard. For NSTS flight operations, a catastrophic hazard is a hazard, which has potential for personal injury, loss of life, loss of the orbiter, or NSTS equipment. For ground operations, a catastrophic hazard is a hazard, which has potential for personnel fatality or loss of the launch site facilities, GSE, payload(s), or orbiter.

A.6 Collected Volatile Condensable Material (CVCM). The quantity of outgassed material from a test specimen that condenses on a collector.

A.7 Component. A combination of parts, devices, or structures that perform a distinctive action or process, or provide support. Examples are transmitter, gyro package, actuator, motor, and battery.

A.8 Configuration. The functional and physical characteristics of parts, assemblies, equipment, or systems, or any combination of these, which are capable of fulfilling the fit, form, and functional requirements defined by performance specifications and engineering drawings.

A.9 Configuration Control. The systematic evaluation, coordination, and formal approval/ disapproval of proposed changes and implementation of all approved changes to the design and production of an item and the configuration of which has been formally approved by the developer or by the purchaser, or both.

A.10 Configuration Management. The systematic control and evaluation of all changes to baseline documentation and subsequent changes to that documentation, which define the original scope of effort to be accomplished (contract and reference documentation) and the systematic control, identification, status accounting, and verification of all configuration items.

A.11 Contamination. The presence of materials of molecular or particulate nature that degrades the performance of hardware.

A.12 Continuous Risk Management (CMR). An organized, systematic decision-making process that efficiently and effectively identifies, analyzes, plans (for the handling of risks), tracks, controls, communicates, and documents risk to increase the likelihood of achieving program/project goals.

A.13 Credible Failure Mode. A failure mode that is possible.

A.14 Critical Hazard. For flight operations, a hazard that has potential for damage to equipment. For ground operations, a hazard that has potential for damage to site facilities.

A.15 De-rating. The reduction of the applied load (or rating) of a device to improve reliability or to permit operation at high ambient temperatures.

A.16 Design Specification. Generic designation for a specification which describes functional and physical requirements for an article, usually at the component level or higher levels of assembly. In its initial form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements. The design specification evolves through the program/project life cycle to reflect progressive refinements in performance, design, configuration, and test requirements. In many program/projects the end-item specifications serve all the purposes of design specifications for the contract end-items. Design specifications provide the basis for technical and engineering management control.

A.17 Designated Representative. An individual (such as a NASA plant representative), firm (such as assessment contractor), Department of Defense (DOD) plant representative, or other government representative designated and authorized by NASA to perform a specific function for NASA. As related to the contractor's effort, this may include evaluation, assessment, design review, participation, and review/approval of certain documents or actions.

A.18 Deviation. A specific authorization granted before the fact to depart from a particular requirement of specifications or related documents.

A.19 Discrepancy. See Nonconformance.

A.20 Electromagnetic Compatibility. When various electronic components are performing in a system according to test requirements.

A.21 Electromagnetic Interference. Electromagnetic energy, which interrupts, obstructs, or otherwise degrades or limits the effective performance of electrical equipment.

A.22 Electromagnetic Susceptibility. Undesired response by a component, subsystem, or system to conducted or radiated electromagnetic emissions.

A.23 Element, ISS. Hardware that is an integral part of the International Space Station (ISS) and not considered a payload.

A.24 Enclosed Payload, Shuttle. A payload located in the crew compartment of the shuttle.

A.25 End-to-End Tests. Tests performed on the integrated ground and flight system, including all elements of the payload, its control, communications, and data processing to demonstrate that the entire system is operating in a manner to fulfill all mission requirements and objectives.

A.26 Expected Failure-Free Life. That period of time following acceptance testing during which an item is not expected to (1) fail catastrophically or (2) degrade in functional output or performance beyond acceptable limits. (Expected failure-free life ***shall*** be determined by supplier/vendor test or field performance data, applicable reliability data sources, or will be estimated by design engineering in the absence of any tabulated data based upon design knowledge, experience, and judgment.)

A.27 Experiment. See Payload.

A.28 Exposed Payload, Shuttle. A payload located in the payload bay of the shuttle.

A.29 Facility, ISS. Also called facility class payload. A payload that has a direct physical interface with the ISS and an expected long utilization life of 10 years.

A.30 Failure. The inability of a system, subsystem, component, or part to perform its required function within specified limits, under specified conditions for a specified duration.

A.31 Failure Mode. A description of the manner in which an item can fail.

A.32 Failure Modes and Effects Analysis (FMEA). A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed to determine the effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

A.33Failure Mode Criticality. The severity of the worst-case effects from a specific failure mode which is expressed by a numerical designator.

A.34 Function. An action or process performed by a subsystem or component, which usually involves the transfer of energy and may include the transfer of information or consumable products. (Note: an alternative definition may apply to passive components of a system such as a structure whose "function" is load bearing capability. Welds, brazing, and epoxy have a function which is to provide adhesion of parts when subjected to forces. Function applies to gaseous fuels and oxygen in that their function is to provide consumable products required to create a combustion event for scientific study.)

A.35 Functional Tests. The operation of a unit in accordance with a defined operational procedure to determine whether performance is within the specified requirements.

A.36 Generic Hazard. Those hazard groups that may be present in the design or use of equipment and generally include hazard causes from the environment, collision, fire/explosion (explosion/implosion) vibration/shock/acoustic effect, thermal effects, contamination, radiation, electrical discharge, biological/physiological/psychological impact, toxicity, and other general items.

A.37 Get Away Special (GAS). Shuttle carrier consisting of a canister that accommodates a small experimental payload.

A.38 Glovebox. An enclosed volume that provides physical isolation of an experiment from its environment and enables crew member manipulation of experiment hardware through glove ports.

A.39 Hardware. As used in this document, there are two major categories of hardware as follows:

a. Prototype Hardware: Hardware of a new design; it is subject to a design qualification test program; it is not intended for flight.

b. Flight Hardware: Hardware to be used operationally in space. It includes the following subsets:

(1) Protoflight Hardware: Flight hardware of a new design; it is subject to a test program that combines elements of prototype and flight acceptance verification; that is, the application of design qualification test levels and flight acceptance test durations.

(2) Follow-On Hardware: Flight hardware built in accordance with a design that has been qualified either as prototype or as protoflight hardware; follow-on hardware is subject to a flight acceptance test program.

(3) Spare Hardware: Hardware the design of which has been proven in a design qualification test program; it is subject to a flight acceptance test program and is used to replace flight hardware that is no longer acceptable for flight.

(4) Reflight Hardware: Flight hardware that has been used operationally in space and is to be reused in the same way; the verification program to which it is subject depends on its past performance, status, and the upcoming mission.

A.40 Hazard. A risk situation that could cause an unsafe condition that could result in an accident.

A.41 Hazard Analysis (HA). The technique used to systematically identify, evaluate, and resolve hazards. The determination of potential sources of danger, causes, effects, hazard levels, and recommended resolution for those conditions found in either the hardware/software system; the person-machine relationship, or both, that could cause loss of life or injury to persons or damage to or loss of systems or equipment.

A.42 Hazard Category. Category used in risk assessment associated with accidents (e.g., low, medium, and high).

A.43 Hitchhiker. A carrier that can carry payloads side mounted in the shuttle payload bay or mounted on a cross-bay "bridge" structure.

A.44 Inspection. The process of comparing an article with requirements.

A.45 Item. Space flight hardware such as a part, component, assembly, or material used to fabricate flight hardware.

A.46 Limited Life Items. Space flight hardware (1) whose failure consequences are safety or mission critical, and (2) has an expected failure-free life that is less than the projected mission time when considering cumulative ground operation, storage, and on-orbit operation (material used to fabricate flight hardware with a shelf life that is less than its planned storage time qualifies as a limited life item).

A.47 Maintainability. A system effectiveness concept that measures the ease and rapidity with which a system or equipment can be restored to operational status after failing.

A.48 Margin. The amount by which hardware capability exceeds mission requirements.

A.49 Monitor. To keep track of the progress of a performance assurance activity; the monitor need not be present at the scene during the entire course of the activity, but he will review resulting data or other associated documentation (see Witness).

A.50 Noncompliance (Safety). If a requirement of NHB 1700.7 or KHB (1700.7) cannot be met, the payload organization must submit a Payload Safety Noncompliance Report. The report contains the rationale and supporting data that demonstrates the safety of the questionable design feature, procedures, configuration, etc. If the NSTS operator approves the noncompliance, the approval will come in the form either of a waiver or a deviation. Waivers restrict the use of the noncomplying feature to a single mission and a single payload element. A deviation may allow the feature to be employed for more than one mission. A deviation applies to a feature that does not comply with a requirement in the specified manner but does satisfy the intent of the requirement and achieves a comparable or higher degree of safety.

A.51 Nonconformance. A condition of any hardware, software, material, or service in which one or more characteristics do not conform to requirements. As applied in quality assurance, nonconformance's fall into two categories—discrepancies and failures. A discrepancy is a departure from specification that is detected during inspection or process control testing, etc., while the hardware or software is not functioning or operating. A failure is a departure from specification that is discovered in the functioning or operation of the hardware or software.

A.52 Offgassing. The emanation of volatile matter of any kind from materials into a manned pressurized volume.

A.53 Outgassing. The spontaneous evolution of gas or vapor from a material, and evolution of the decomposition products, in a vacuum.

A.54 Part. A hardware element that is not normally subject to further subdivision or disassembly without destruction of designed use.

A.55 Payload. An integrated assemblage of subsystems designed to perform a specified mission in space.

A.56 Payload, ISS. Equipment designed and developed for the purpose of performing research onboard the ISS that is not considered part of the space station system. ISS payloads are classified as Facility Class (see Facility, ISS), Complex Subrack/Subpallet Class, and Subrack/Subpallet Class.

A.57 Performance Verification. Determination by test, analysis, or a combination of the two that the payload element can operate as intended in a particular mission; this includes being satisfied that the design of the payload or element has been qualified and that the particular item has been accepted as true to the design and ready for flight operations.

A.58 Performance Measure. It is a metric which characterizes the performance of a system, process, or activity in fulfilling its intended objectives.

A.59 Preliminary Hazard Analysis. An analysis technique for performing an initial risk assessment of a system concept to identify safety-critical areas, evaluate hazards, and identify the safety design requirements needed in the program/project.

A.60 Primary Payload, ELV. The payload that is the primary mission of the launch vehicle.

A.61 Prototype Hardware. See Hardware.

A.62 Qualification Tests. The process of demonstrating that a given design and manufacturing approach will produce hardware that will meet all performance specifications when subjected to defined conditions more severe than those expected to occur during its intended use.

A.63 Radiation Hardness. The ability of a system, subsystem, or component to perform the intended functions when exposed to the radiation levels in the space environment for the mission.

A.64 Redundancy (of design). The use of more than one independent means of accomplishing a given function.

A.65 Reliability. The probability that a system, subsystem, or component can perform its intended function for a specified interval of time under stated conditions.

A.66 Repair. A corrective maintenance action performed as a result of a failure so as to restore an item to operation within specified limits.

A.67 Rework. Return for completion of operations (complete to drawing). The article is to be reprocessed to conform to the original specifications or drawings.

A.68 Risk. The combination of (1) the probability (qualitative or quantitative) that a program or project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, compromise of security, or failure to achieve a needed technological breakthrough and (2) the consequences, impact, or severity of the undesired event were it to occur.

A.69 Risk Informed Decision Making (RIDM). The RIDM fosters development of the most robust technical basis for decision making by blending risk and traditional metrics, seeking to capitalize on the strengths of both while avoiding their pitfalls. The RIDM incorporates a deliberative process intended to capitalize on tacit organizational knowledge after the analysis/modeling stage.

A.70 Secondary Payload, ELV. A smaller payload launched along with the primary payload and taking advantage of the launch vehicle’s excess payload capability.

A.71 Similarity, Verification By. A procedure of comparing an item to a similar one that has been verified. Configuration, test data, application, and environment should be evaluated. It should be determined that design differences are insignificant, environmental stress will not be greater in the new application, and that manufacturer and manufacturing methods are the same.

A.72 Single Point Failure. A single element of hardware the failure of which would result in loss of mission objectives, hardware, or crew, as defined for the specific application or program/project for which a single point failure analysis is performed.

A.73 Subassembly. A subdivision of an assembly. Examples are wire harness and loaded printed circuit boards.

A.74 Subsystem. A functional subdivision of a payload consisting of two or more components. Examples are attitude control, electrical power subsystems, and instruments.

A.75 Technology Readiness Level (TRL). A measure of the risk for a program/project that chooses to use a new technology. The TRL scale ranges from 1 to 9. A TRL=9 is used for existing, well-established, proven (very low-risk) technology. A TRL=1 is used for unproven, very high-risk technology at the basic research stage.

A.76 Temperature Cycle. A transition from some initial temperature condition to temperature stabilization at one extreme and then to temperature stabilization at the opposite extreme and returning to the initial temperature condition.

A.77 Temperature Stabilization. The condition that exists when the rate of change of temperatures has decreased to the point where the test item may be expected to remain within the specified test tolerance for the duration or where further change is considered acceptable.

A.78 Thermal Balance Test. A test conducted to verify the adequacy of the thermal design and the capability of the thermal control system to maintain thermal conditions within established mission limits.

A.79 Thermal-Vacuum Test. The thermal balance test is often part of a system level thermal vacuum test and performed on flight hardware. It can also be conducted at subsystem and lower levels as needed. The test provides data for transient and steady state correlation of analytic thermal models and verifies adequacy of the thermal design and thermal control system. Thermal balance tests typically incorporate worst case hot and cold mission scenarios as a minimum.

A.80 Total Mass Loss (TML). Total mass of material outgassed from a specimen that is maintained at a specified constant temperature and operating pressure for a specified time.

A.81 Verification. See Performance Verification.

A.82 Vibroacoustics. An environment induced by high-intensity acoustic noise associated with various segments of the flight profile; it manifests itself throughout the payload in the form of directly transmitted acoustic excitation and as structure-borne random vibration excitation.

A.83 Waiver. A written authorization granting use or acceptance of an article which does not meet specified requirements. A waiver is authorized after the fact.

A.84 Witness. A personal, on-the-scene observation of a performance assurance activity with the purpose of verifying compliance with program/project requirements (see Monitor).

Appendix B. Acronyms

B.1 ABPL. As-Built Parts List
B.2 ADP. Acceptance Data Package
B.3 ADPL. As-Designed Parts List
B.4 AIAA. American Institute of Aeronautics and Astronautics
B.5 AIT. Assembly, Inspection and Test
B.6 ANSI. American National Standards Institute
B.7 ASME. American Society of Mechanical Engineers
B.8 ASTM. American Society for Testing and Materials
B.9 ATD. Advanced Technology Development
B.10 ATV. Automated Transfer Vehicle
B.11 AWS. American Welding Society
B.12 BMS. Business Management System
B.13 CAGE. Commercial and Government Entity
B.14 CCB. Configuration Control Board
B.15 CCP. Contamination Control Plan
B.16 CDR. Critical Design Review
B.17 CIL. Critical Items List
B.18 CM. Configuration Management
B.19 CoFR. Certificate of Flight Readiness
B.20 CORR. Corrosion Resistance
B.21 COTS. Commercial Off-the-Shelf
B.22 CPARS. Corrective and Preventative Action Reporting System
B.23 CRM. Continuous Risk Management
B.24 CSCI. Computer Software Configuration Item
B.25 CSO. Chief Safety and Mission Assurance Officer
B.26 CVCM. Collected Volatile Condensable Material
B.27 DFMR. Design for Minimum Risk
B.28 ECO. Engineering Change Order
B.29 ECR. Engineering Change Request
B.30 EDMS. Electronic Document Management System
B.31 EEE. Electrical, Electronic and Electromechanical
B.32 ELDRS. Enhanced Low Dose Rate Sensitivity
B.33 ELV. Expendable Launch Vehicle
B.34 EMC. Electromagnetic Compatibility
B.35 EMI. Electromagnetic Interference
B.36 ERRIC. Electronics Radiation Response Information Center
B.37 ESD. Electrostatic Discharge

B.38 EVA. Extra-Vehicular Activity
B.39 FAR. Federal Acquisition Regulation
B.40 FCA. Functional Configuration Audit
B.41 FHA. Functional Hazard Analysis
B.42 FLAM. Flammability
B.43 FMEA. Failure Modes and Effects Analysis
B.44 FS. Factor of Safety
B.45 FSC. Fluid System Compatibility
B.46 FS&GS. Flight Systems and Ground Support
B.47 GAS. Get Away Special
B.48 GB. Glove Box
B.49 GIDEP. Government-Industry Data Exchange Program
B.50 GLPD. Glenn Policy Directive
B.51 GLPR. Glenn Procedural Requirements
B.52 GMIP. Government Mandatory Inspection Points
B.53 GOX. Gaseous Oxygen
B.54 GRC. Glenn Research Center
B.55 GSE. Ground Support Equipment
B.56 GSFC. Goddard Space Flight Center
B.57 GSRP. Ground Safety Review Panel
B.58 HTV. H-II Transfer Vehicle
B.59 ICA. Inter Center Agreement
B.60 IHA. Integrated Hazard Analysis
B.61 IPC. Institute for Interconnecting and Packaging Electronic Circuits
B.62 IRIS. Incident Reporting Information System
B.63 ISS. International Space Station
B.64 IVA. Intra-Vehicular Activity
B.65 JPL. Jet Propulsion Laboratory
B.66 JSC. Johnson Space Center
B.67 KSC. Kennedy Space Center
B.68 LET. Linear Energy Transfer
B.69 LOX. Liquid Oxygen
B.70 LRU. Line Replaceable Unit
B.71 M&P. Materials and Processes
B.72 MAPTIS. Materials and Processes Technical Information System
B.73 MDP. Maximum Design Pressure
B.74 MEFL. Maximum Expected Flight Level
B.75 MIL-STD. Military Standard
B.76 MIUL. Material Identification and Usage List
B.77 MS. Margin of Safety

B.78 MSFC. Marshall Space Flight Center
B.79 MSG. Microgravity Science Glovebox
B.80 MTBF. Mean Time between Failure
B.81 MTTR. Mean Time to Repair, Restore or Replace
B.82 MUA. Materials Usage Agreement
B.83 NDE. Nondestructive Evaluation
B.84 NEPAG. NASA EEE Parts Assurance Group
B.85 NEPP. NASA Electronics Parts and Packaging Program
B.86 NFS. NASA Federal Acquisition Regulation Supplement
B.87 NPD. NASA Policy Directive
B.88 NPR. NASA Procedural Requirement
B.89 NPSL. NASA Parts Selection List
B.90 NSTS. National Space Transportation System (Shuttle)
B.91 ORU. Orbital Replaceable Unit
B.92 O&SHA. Operating and Support Hazard Analysis
B.93 PAP. Project Assurance Plan
B.94 PCA. Physical Configuration Audit
B.95 PCE. Project Chief Engineer
B.96 PDR. Preliminary Design Review
B.97 PHA. Preliminary Hazard Analysis
B.98 PIL. Parts Identification List
B.99 PM. Project Manager
B.100 PPAD. Program and Project Assurance Division
B.101 PPL. Preferred Parts List
B.102 PRA. Probabilistic Risk Assessment
B.103 PRACA. Problem Reporting and Corrective Action
B.104 PSR. Pre-Ship Review
B.105 PSRP. Payload Safety Review Panel
B.106 QA. Quality Assurance
B.107 R&M. Reliability and Maintainability
B.108 RAM. Reliability, Availability and Maintainability
B.109 RFCB. Responsible Fracture Control Board
B.110 RIDM. Risk Informed Decision Making
B.111 RMIT. Risk Management Implementation Tool
B.112 RM. Risk Management
B.113 RSS. Root-Sum-Square
B.114 SA. Software Assurance
B.115 SAGE. Standard Assurance Guidelines for Experiments
B.116 SAR. Space Assurance Requirements
B.117 SARGE. Space Assurance Requirements and Guidelines for Experiments

B.118 SAWE. Society of Allied Weight Engineers
B.119 SBIR. Small Business Innovation Research
B.120 SCC. Stress Corrosion Cracking
B.121 SCD. Source Control Drawing
B.122 SCMP. Software Configuration Management Plan
B.123 SCS. Safety-Critical Structures
B.124 SDF. Software Development Folder
B.125 SDP. Safety Data Package
B.126 SEE. Single Event Effects
B.127 SE&I. Systems Engineering and Integration
B.128 SEMP. Systems Engineering Management Plan
B.129 SHA. System Hazard Analysis
B.130 SMA. Safety and Mission Assurance
B.131 SMAD. Safety and Mission Assurance Directorate
B.132 SMAP. Safety and Mission Assurance Plan
B.133 SMARTS. Safety and Mission Assurance Requirements Tracking System
B.134 SR&QA. Safety, Reliability and Quality Assurance
B.135 SSHA. Subsystem Hazard Analysis
B.136 SSTP. System Safety Technical Plan
B.137 STS. Space Transportation System (Shuttle)
B.138 SWHA. Software Hazard Analysis
B.139 TID. Total Ionizing Dose
B.140 TML. Total Mass Loss
B.141 TOX. Toxicity
B.142 TRL. Technology Readiness Level
B.143 TVS. Thermal Vacuum Stability
B.144 VRR. Verification Readiness Review
B.145 V&V. Verification and Validation
B.146 WFF. Wallops Flight Facility

Appendix C. Verification Matrix

a. Verification to Space Assurance Requirements (SAR) ***shall*** be satisfied by successful completion of the program and project reviews, verification as defined in the Safety and Mission Assurance Plan, and release of the associated data products listed in the contract. This table provides a cross-reference matrix to the SAR and the project verification method.

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
1.	2.1	Description of Overall Requirements				
2.	2.2	Safety and Mission Assurance Plan				
3.	2.2.1	Use of Deviations				
4.	2.3	Use of Previously Designed, Fabricated or Flown Systems				
5.	2.3.1	Storage Requirements for Suspended Projects				
6.	2.4	Assurance Status Reports				
7.	2.5	Contractor Surveillance				
8.	2.6	GRC Assurance Review Requirements				
9.	3.1	Verification General Requirements				
10.	3.2	Overall Verification Program				
11.	3.3	Electrical Verification Requirements				
12.	3.4	Structural and Mechanical Requirements				
13.	3.4.1	Safety Critical and Fracture Critical Structures				
14.	3.4.2	Structural Loads				
15.	3.4.3	Factors of Safety				
16.	3.4.4	Margins of Safety				
17.	3.4.5	Fracture Control				
18.	3.4.6	Pressurized Systems				
19.	3.4.7	Strength Testing				
20.	3.4.8	Vibroacoustics				
21.	3.4.8.1	Component Random Vibration Testing				
22.	3.4.8.1.1	Workmanship				
23.	3.4.8.1.2	Stowed Components				
24.	3.4.8.1.3	Retesting of Reflight Vibration Testing				
25.	3.4.8.2	Additional Vibroacoustic Testing				
26.	3.4.9	Shock (Mechanical Pyro)				
27.	3.4.9.1	Flight Acceptance				
28.	3.4.10	Mechanical Functions				

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
29.	3.4.10.1	Qualification Testing				
30.	3.4.10.2	Flight Acceptance Testing				
31.	3.4.11	Pressure Profile				
32.	3.4.12	Fastener Integrity				
33.	3.4.13	Mass Properties				
34.	3.4.14	Ground Support Equipment				
35.	3.5	Electromagnetic Compatibility (EMC) Requirements				
36.	3.6	Radiation Requirements				
37.	3.7	Vacuum, Thermal, and Humidity Requirements				
38.	3.7.1	Compliance With Requirements				
39.	3.7.2	Testing Levels				
40.	3.7.3	Description of Applicable Testing				
41.	3.7.4	Description of Applicable Analysis				
42.	3.8	Flight System Performance Acceptance Test Requirements				
43.	3.8.1	Burn-in Tests				
44.	3.8.2	Mission Simulation Test				
45.	3.8.3	End-to-End Compatibility Test				
46.	4.1	System Safety Introduction				
47.	4.2	System Safety Planning				
48.	4.2.1	System Safety Assurance Reviews				
49.	4.3	Hazards Analysis				
50.	4.4	Failure Tolerance				
51.	4.5	Design of Minimum Risk				
52.	4.6	Internal GRC Review of Safety Products				
53.	4.7	Requirements Applicability				
54.	5.1	Parts General Requirements				
55.	5.2	EEE Parts Selection and Screening				
56.	5.2.1	EEE Parts Control Plan				
57.	5.2.2	EEE Parts Selection and Grade				
58.	5.2.3	Flight EEE Parts Qualification				
59.	5.2.4	Flight EEE Parts Screening				
60.	5.2.5	De-rating				
61.	5.2.6	Radiation Hardness				
62.	5.2.7	Corona and Arcing				
63.	5.3	Mechanical Parts Selection and Screening				

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
64.	5.3.1	Mechanical Parts Control Plan				
65.	5.3.2	Inspection Prior to Assembly				
66.	5.4	Procurement of Parts				
67.	5.4.1	Parts Obsolescence and Diminishing Manufacturing Sources				
68.	5.5	Parts Storage Control				
69.	5.6	Parts Age Control				
70.	5.7	Parts Identification List				
71.	5.8	Parts Risk Evaluation				
72.	5.9	Parts Subject to Metal Whisker Growth				
73.	6.1	M&P General Requirements				
74.	6.2	Safety and Mission Assurance Plan Specific Requirements				
75.	7.1.2	RAM Requirement for an Integrated Process				
76.	7.1.3	RAM Management				
77.	7.1.4	RAM Plan				
78.	7.1.5	RAM Data				
79.	7.1.6	RAM Reports Archives				
80.	7.1.7	Reliability and Failure Tolerance				
81.	7.2.1	PRA General Requirements				
82.	7.2.2	Criteria for PRA Decision				
83.	7.2.3	PRA Objectives and Ground Rules				
84.	7.2.4	Application of PRA				
85.	7.2.5	Requirement for an Integrated Process				
86.	7.2.6	PRA Management				
87.	7.2.7	PRA Plan				
88.	8.1	QA General Requirements				
89.	8.2	Quality Assurance Organization				
90.	8.3	Configuration Management and Verification				
91.	8.4	Identification and Traceability				
92.	8.5	Procurement Requirements				
93.	8.5.1	Government Source Inspection				
94.	8.5.2	Receiving Inspection				
95.	8.6	Control of Fabrication Activities				
96.	8.6.1	Fabrication and Inspection Requirements				
97.	8.6.1.1	Control of Assembly, Inspection, and Test Activities				
98.	8.6.1.2	Assembly, Inspection and Test (AIT) Procedures				
99.	8.6.2	Training for Personnel				

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
100.	8.6.3	Evaluation and Control of Process Specifications and Procedures				
101.	8.6.4	Bonded Storage				
102.	8.6.5	Records of Inspections and Tests				
103.	8.7	Contamination Control				
104.	8.7.1	Contamination Control Plan				
105.	8.8	Electrostatic Discharge Prevention				
106.	8.9	Nonconformance and Problem Reporting and Control				
107.	8.9.1	Review Boards				
108.	8.9.2	Waivers and Deviations				
109.	8.10	Alert Information				
110.	8.11	Inspection and Test of Stored Limited-Life Hardware				
111.	8.12	Metrology				
112.	8.13	Handling, Preservation, Marking, Packaging, Packing and Transportation				
113.	8.13.1	Control of Government Property by Contractors				
114.	8.14	Configuration Verification				
115.	8.15	Acceptance of Flight System				
116.	8.16	Quality Program Audits				
117.	8.17	Control of Quality Records				
118.	9.3	Risk General Requirements				
119.	9.4	Initial Risk Management Training				
120.	9.5	Implementation				
121.	9.5.1	Identify Risks				
122.	9.5.2	Analyze Risks				
123.	9.5.3	Planning				
124.	9.5.4	Risk Tracking				
125.	9.5.5	Risk Control				
126.	9.5.6	Communication and Documentation				
127.	10.1	Software General Requirements				
128.	10.1.1	Roles and Responsibilities				
129.	10.1.2	Scope of Software Assurance Activities				
130.	10.2	Software Safety				
131.	10.3	Software Reliability				
132.	10.4	Software Configuration Management				
133.	10.5	Software Nonconformance Reporting and Corrective Action				
134.	10.6	Software Verification and Validation				

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
135.	10.6.1	Software Review				
136.	10.6.2	Software Inspections				
137.	10.6.3	Software System Testing				
138.	10.6.4	Software Audits				
139.	10.6.5	Software Acceptance				

Appendix D. Templates and Forms

D.1 Safety and Mission Assurance Plan Template

National Aeronautics and
Space Administration

Document Number
Revision Status: *Draft/Baseline/Revision*
Effective Date: April 9, 2009

John H. Glenn Research Center at Lewis Field
21000 Brookpark Road, Cleveland, Ohio 44135

GRC Safety and Mission Assurance Plan (SMAP)

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 2 of 18

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Draft			Draft

Instructions for Filling Out This Template

Note that this, and all subsequent text in italics, provides instructions for filling out this template. This template is provided as a guide to generate Project Plans and is intended to be tailored to fit the specific Glenn Research Center (GRC) project or program. These instructions should be removed prior to publishing the plan.

Safety and Mission Assurance Plan, SMAP, Document Number and date are hyperlinked throughout the document to the title page. On the title page, double-click these items and enter the appropriate text. Once each of these items has been entered, go to the Edit menu, then select "Links," select all of the links, and click "Update."

The Table of Contents is also linked. To update, simply right-mouse click, select "Update field," and then select "Update entire table." Please note that the document is also set to automatically update as it is printed.

This template represents a skeletal outline of a Project Plan. The actual plan should reflect the scope and needs of the project. The need to correctly identify only the required tasks to suit the project cannot be overstated. If any tasks in this template are determined "not applicable" on large or small programs or projects, the paragraph will be identified as "not applicable" or you may delete the tasks. If tasks in this template are determined to be missing, please add them and inform the GLPR 7123.22 author so that appropriate updates can be made as necessary.

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)

Signature Page

PREPARED BY:

SMAP Q Representative — Date
<Full name with initials>
Glenn Research Center

CONCURRED BY:

SMAP Project Management — Date
Engineering Directorate
Glenn Research Center

SMAP Code D Management — Date
Engineering Directorate
Glenn Research Center

SMAP Code Q Management — Date
Safety & Mission Assurance Directorate
Glenn Research Center

SMAP Code M Management — Date
Space Flight Systems Directorate
Glenn Research Center

APPROVED BY:

SMAP *<Project Customer>* — Date
<Full name with initials>
<Center>

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 4 of 18

Contents

1.0 Project Overview 7
1.1 Introduction 7
1.2 Objectives 7
1.3 Mission Description and Technical Approach 7
1.4 Project Authority, Governance Structure, Management Structure, and Implementation Approach 7
2.0 Documents 7
2.1 Applicable Documents 7
2.2 Reference Documents 7
2.3 Overall Requirements 7
2.4 Reference Documents 7
2.5 Reference Documents 7
3.0 Design and Verification 7
3.1 General Requirements 7
3.2 Overall Verification Program 7
3.3 Electrical Verification Requirements 7
3.4 Structural and Mechanical Requirements 8
3.5 Electromagnetic Compatibility (EMC) Requirements 8
3.6 Radiation Requirements 8
3.7 Vacuum, Thermal, and Humidity Requirements 8
3.8 Flight System Performance Acceptance Test Requirements 8
4.0 System Safety 8
4.1 Introduction 8
4.2 System Safety Planning 8
4.3 Hazards Analysis 8
4.4 Failure Tolerance 8
4.5 Design for Minimum Risk 8
4.6 Internal GRC Review of Safety Products 8
4.7 Requirements Applicability 8
5.0 EEE and Mechanical Parts Control 9
5.1 General Requirements 9
5.2 EEE Parts Selection and Screening 9
5.2.1 EEE Parts Control Plan 9
5.2.2 EEE Parts Selection and Grade 9
5.2.3 Flight EEE Parts Qualification 9
5.2.4 Flight EEE Parts Screening 9
5.2.5 De-rating 9
5.2.6 Radiation Hardness 9
5.2.7 Corona and Arcing 9
5.2.8 Inspection Prior to Assembly 9
5.3 Mechanical Parts Selection and Screening 9
5.3.1 Mechanical Parts Control Plan 9
5.3.2 Inspection Prior to Assembly 9

D.1 Safety and Mission Assurance Plan Template (con't)

5.4 Procurement of Parts 9
5.4.1 Parts Obsolescence and Diminishing Manufacturing Sources 9
5.5 Parts Storage Control 9
5.6 Parts Age Control 9
5.7 Parts Identification List 10
5.8 Parts Risk Evaluation 10
5.9 Parts Subject to Metal Whisker Growth 10
6.0 Materials and Processes Requirements 10
6.1 General Requirements 10
6.2 Safety and Mission Assurance Plan Specific Requirements 10
7.0 Reliability and Probabilistic Risk Assessment 10
7.1 Reliability, Availability, and Maintainability 10
7.1.1 General Requirements 10
7.1.2 Requirement for an Integrated Process 10
7.1.3 RAM Management 10
7.1.4 RAM Plan 10
7.1.5 RAM Data 10
7.1.6 RAM Reports Archives 10
7.1.7 Reliability and Failure Tolerance 10
7.2 Probabilistic Risk Assessment 10
7.2.1 General Requirements 10
7.2.2 Criteria for PRA Decision 10
7.2.3 PRA Objectives and Ground Rules 11
7.2.4 Application of PRA 11
7.2.5 Requirement for an Integrated Process 11
7.2.6 PRA Management 11
7.2.7 PRA Plan 11
8.0 Quality Assurance Requirements 11
8.1 General Requirements 11
8.2 Quality Assurance Organization 11
8.3 Configuration Management and Verification 11
8.4 Identification and Traceability 11
8.5 Procurement Requirements 11
8.5.1 Government Source Inspection 11
8.5.2 Receiving Inspection 11
8.6 Control of Fabrication Activities 11
8.6.1 Fabrication and Inspection Requirements 11
8.6.2 Training for Personnel 11
8.6.3 Evaluation and Control of Process Specifications and Procedures 11
8.6.4 Bonded Storage 11
8.6.5 Records of Inspection and Tests 11
8.7 Contamination Control 12
8.7.1 Contamination Control Plan 12
8.8 Electrostatic Discharge Prevention 12
8.9 Nonconformance and Problem Reporting and Control 12

D.1 Safety and Mission Assurance Plan Template (con't)

8.9.1 Review Boards 12
8.9.2 Waivers and Deviations 12
8.10 Alert Information 12
8.11 Inspection and Test of Stored Limited-Life Hardware 12
8.12 Metrology 12
8.13 Handling, Preservation, Marking, Packaging, Packing, and Transportation 12
8.13.1 Control of Government Property by Contracts 12
8.14 Configuration Verification 12
8.15 Acceptance of Flight Systems 12
8.16 Quality Program Audits 12
8.17 Control of Quality Records 13
9.0 Continuous Risk Management 14
9.1 Risk 14
9.2 Introduction 14
9.2.1 Risk Informed Decision Making (RIDM) 14
9.2.2 Continuous Risk Management (CRM) 14
9.2.3 RIDM and CRM 14
9.2.4 Institutional Risks 14
9.3 General Requirements 14
9.4 Initial Risk Management Training 14
9.5 Implementation 14
9.5.1 Identify Risks 14
9.5.2 Analyze Risks 14
9.5.3 Planning 14
9.5.4 Risk Tracking 14
9.5.5 Risk Control 14
9.5.6 Communication and Documentation 14
10.0 Software Assurance 14
10.1 General Requirements 14
10.1.1 Roles and Responsibilities 14
10.1.2 Scope of Software Assurance Activities 14
10.2 Software Safety 14
10.3 Software Reliability 15
10.4 Software Configuration Management 15
10.5 Software Nonconformance Reporting and Corrective Action 15
10.6 Software Verification and Validation 15
10.6.1 Software Review 15
10.6.2 Software Inspections 15
10.6.3 Software System Testing 15
10.6.4 Software Audits 15
10.6.5 Software Acceptance 15
Appendix A —Verification Matrix 16

List of Figures

List of Tables

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 7 of 18

1.0 Project Overview

1.1 Introduction

a. *Briefly describe the background of the project and its current status, including results of formulation activities, decisions, and documentation.*

1.2 Objectives

a. *State the specific project goals and objectives.*

1.3 Mission Description and Technical Approach

a. *Describe the mission that the project supports and the project role in the mission.*

1.4 Project Authority, Governance Structure, Management Structure, and Implementation Approach

a. *Provide a brief technical description of the product/deliverable/output of this project. Describe the systems to be developed and the basic operations concept. Describe the development approach to systems, subsystems, and components with regard to design maturation and hardware/software development levels (breadboard, engineering, qualification, protoflight, prototype, and flight).*

2.0 Documents

2.1 Applicable Documents

2.2 Reference Documents

2.3 Overall Requirements

a. *Provide a description of how this project is planning to meet the requirements of Chapter 2.*

2.4 Reference Documents

2.5 Reference Documents

3.0 Design and Verification

3.1 General Requirements

a. *Provide a description of the project's verification approach.*

3.2 Overall Verification Program

a. *Provide a description of the project's verification program.*

b. *Provide a link to the project verification plan.*

3.3 Electrical Verification Requirements

a. *Provide a description of how the project plans to meet the electrical verification requirements.*

D.1 Safety and Mission Assurance Plan Template (con't)

3.4 Structural and Mechanical Requirements

a. *Provide a description of how the project plans to meet each of the structural and mechanical requirements.*

3.5 Electromagnetic Compatibility (EMC) Requirements

a. *Provide a description of how the project plans to meet each of the EMC requirements.*

3.6 Radiation Requirements

a. *Provide a description of how the project plans to meet the radiation requirements.*

3.7 Vacuum, Thermal, and Humidity Requirements

a. *Provide a description of how the project plans to meet each of the vacuum, thermal, and humidity requirements.*

3.8 Flight System Performance Acceptance Test Requirements

a. *Provide a description of how the project plans to meet each of the Flight System Performance Acceptance Test requirements.*

4.0 System Safety

4.1 Introduction

4.2 System Safety Planning

a. *Provide a description of the project's System Safety Technical approach.*

b. *Provide a description of how the project plans to meet each of the System Safety Planning requirements.*

4.3 Hazards Analysis

a. *Provide a description of how the project plans to meet the Hazards Analysis requirements.*

4.4 Failure Tolerance

a. *Provide a description of how the project plans to meet the Failure Tolerance requirements.*

4.5 Design for Minimum Risk

a. *Provide a description of how the project plans to meet the Design for Minimum Risk requirements.*

4.6 Internal GRC Review of Safety Products

a. *Provide a description of how to process the project plans to have the required review and approval/concurrence by the GRC Safety and Mission Assurance Directorate.*

4.7 Requirements Applicability

a. *Provide a list of safety requirements documents that are applicable to the project.*

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 9 of 18

5.0 EEE and Mechanical Parts Control

5.1 General Requirements

a. *Provide a description of how the project plans to meet the Electrical, Electronic, and Electromechanical (EEE) and Mechanical Parts Control Program requirements.*

5.2 EEE Parts Selection and Screening

a. *Provide a description of how the project plans to meet the Electrical, Electronic, and Electromechanical (EEE) and Mechanical Parts Control Program requirements. paragraph.*

5.2.1 EEE Parts Control Plan

5.2.2 EEE Parts Selection and Grade

5.2.3 Flight EEE Parts Qualification

5.2.4 Flight EEE Parts Screening

5.2.5 De-rating

5.2.6 Radiation Hardness

5.2.6.1 **Total Ionizing Dose**
5.2.6.2 **Single Event Effects**
5.2.6.3 **Displacement Damage**

5.2.7 Corona and Arcing

5.2.8 **Inspection Prior to Assembly**

5.3 Mechanical Parts Selection and Screening

a. *Provide a description of how the project plans to meet the Mechanical Parts Selection and Screening requirements.*

5.3.1 Mechanical Parts Control Plan

5.3.2 Inspection Prior to Assembly

5.4 Procurement of Parts

a. *Provide a description of how the project plans to meet the Procurement of Parts requirements*

5.4.1 Parts Obsolescence and Diminishing Manufacturing Sources

5.5 Parts Storage Control

5.6 Parts Age Control

a. *Provide a description of how the project plans to meet the parts age control requirements.*

D.1 Safety and Mission Assurance Plan Template (con't)

5.7 Parts Identification List

a. *Provide a description of how the project plans to meet the parts identification list requirements.*

5.8 Parts Risk Evaluation

a. *Provide a description of how the project plans to meet the parts risk evaluation requirements.*

5.9 Parts Subject to Metal Whisker Growth

a. *Provide a description of how the project plans to meet the parts subject to metal whisker growth requirements.*

6.0 Materials and Processes Requirements

6.1 **General Requirements**

a. *Provide a description of how the project plans to meet the general materials and processes requirements.*

6.2 **Safety and Mission Assurance Plan Specific Requirements**

a. *Provide a description of how the project plans to control materials and processes and meet the specific requirements.*

7.0 Reliability and Probabilistic Risk Assessment

7.1 **Reliability, Availability, and Maintainability**

a. *Provide a description of how the project plans to meet the Reliability, Availability, and Maintainability requirements.*

7.1.1 General Requirements

7.1.2 Requirement for an Integrated Process

7.1.3 RAM Management

7.1.4 RAM Plan

7.1.5 RAM Data

7.1.6 RAM Reports Archives

7.1.7 Reliability and Failure Tolerance

7.1.7.1 **Variances From Two-Failure Tolerance Requirement**

7.2 **Probabilistic Risk Assessment**

a. *Provide a description of how the project plans to meet the Probabilistic Risk Assessment requirements paragraphs.*

7.2.1 General Requirements

7.2.2 Criteria for PRA Decision

D.1 Safety and Mission Assurance Plan Template (con't)

7.2.3 PRA Objectives and Ground Rules

7.2.4 Application of PRA

7.2.5 Requirement for an Integrated Process

7.2.6 PRA Management

7.2.7 PRA Plan

8.0 Quality Assurance Requirements

8.1 General Requirements

a. *Provide a description of how the project plans to meet the general quality assurance requirements.*

8.2 Quality Assurance Organization

a. *Designate the individual responsible for directing and managing the Quality Assurance Program.*

8.3 Configuration Management and Verification

a. *Provide a description of how the project plans to meet the configuration management and verification requirements.*

8.4 Identification and Traceability

a. *Provide a description of how the project plans to meet the identification and traceability requirements.*

8.5 Procurement Requirements

a. *Provide a description of how the project plans to meet the procurement requirements.*

8.5.1 Government Source Inspection

8.5.2 Receiving Inspection

8.6 Control of Fabrication Activities

a. *Provide a description of how the project plans to meet the control of fabrication activities requirements.*

8.6.1 Fabrication and Inspection Requirements

8.6.1.1 **Control of Assembly, Inspection, and Test Activities**
8.6.1.2 **Assembly, Inspection, and Test (AIT) Procedures**

8.6.2 Training for Personnel

8.6.3 Evaluation and Control of Process Specifications and Procedures

8.6.4 Bonded Storage

8.6.5 Records of Inspection and Tests

D.1 Safety and Mission Assurance Plan Template (con't)

8.7 Contamination Control

a. *Provide a description of how the project plans to meet the contamination control requirements.*

8.7.1 Contamination Control Plan

8.8 Electrostatic Discharge Prevention

a. *Provide a description of how the project plans to prevent electrostatic discharge damage to any susceptible parts or components.*

8.9 Nonconformance and Problem Reporting and Control

a. *Provide a description of how the project plans to meet the nonconformance and problem reporting and control requirements.*

8.9.1 Review Boards

8.9.2 Waivers and Deviations

8.10 Alert Information

a. *Provide a description of how the project plans to meet the alert information requirements.*

8.11 Inspection and Test of Stored Limited-Life Hardware

a. *Provide a description of how the project plans to meet the Inspection and Test of Stored Limited-Life Hardware requirements.*

8.12 Metrology

a. *Provide a description of how the project plans to meet the metrology requirements.*

8.13 Handling, Preservation, Marking, Packaging, Packing, and Transportation

a. *Provide a description of how the project plans to meet the handling, preservation, marking, packaging, packing, and transportation requirements.*

8.13.1 Control of Government Property by Contracts

8.14 Configuration Verification

a. *Provide a description of how the project plans to meet the configuration verification requirements.*

8.15 Acceptance of Flight Systems

a. *Provide a description of how the project plans to meet the acceptance of flight systems requirements.*

8.16 Quality Program Audits

a. *Provide a description of how the project plans to meet the quality program audits requirements.*

8.17 Control of Quality Records

a. *Provide a description of how the project plans to meet the control of quality records requirements.*

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 14 of 18

9.0 Continuous Risk Management

9.1 **Risk**

a. *This entire section can be eliminated if the project develops a separate Risk Management Plan that meets the requirements of Chapter 9.*

9.2 **Introduction**

9.2.1 Risk Informed Decision Making (RIDM)

9.2.2 Continuous Risk Management (CRM)

9.2.3 RIDM and CRM

9.2.4 **Institutional Risks**

9.3 **General Requirements**

a. *Provide a description of how the project plans to meet the general risk requirements.*

9.4 **Initial Risk Management Training**

a. *Provide a description of how the project plans to use risk management training within the project.*

9.5 **Implementation**

a. *Provide a description of how the project plans to meet the risk implementation requirements.*

9.5.1 Identify Risks

9.5.2 Analyze Risks

9.5.3 Planning

9.5.4 Risk Tracking

9.5.5 Risk Control

9.5.6 Communication and Documentation

9.5.6.1 **Risk Database**
9.5.6.2 **Risk Reporting**

10.0 Software Assurance

10.1 **General Requirements**

a. *Provide a description of how the project plans to meet the general software requirements.*

10.1.1 Roles and Responsibilities

10.1.2 **Scope of Software Assurance Activities**

10.2 **Software Safety**

a. *Provide a description of how the project plans to meet the software safety requirements.*

D.1 Safety and Mission Assurance Plan Template (con't)

10.3 **Software Reliability**

a. *Provide a description of how the project plans to meet the software reliability requirements.*

10.4 **Software Configuration Management**

a. *Provide a description of how the project plans to meet the software configuration management requirements.*

10.5 **Software Nonconformance Reporting and Corrective Action**

a. *Provide a description of how the project plans to meet the software nonconformance reporting and corrective action requirements.*

10.6 **Software Verification and Validation**

a. *Provide a description of how the project plans to meet the software verification and validation requirements.*

10.6.1 Software Review

10.6.2 Software Inspections

10.6.3 Software System Testing

10.6.4 Software Audits

10.6.5 Software Acceptance

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 16 of 18

Appendix A—Verification Matrix

Verification to Space Assurance Requirements (SAR) ***shall*** be satisfied by successful completion of the program and project reviews, verification as defined in the Safety and Mission Assurance Plan, and release of the associated data products listed in the contract. This table provides a cross-reference matrix to the SAR and the project verification method.

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						
23.						
24.						
25.						
26.						
27.						
28.						
29.						
30.						
31.						
32.						
33.						
34.						
35.						
36.						
37.						
38.						
39.						
40.						
41.						
42.						

D.1 Safety and Mission Assurance Plan Template (con't)

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
43.						
44.						
45.						
46.						
47.						
48.						
49.						
50.						
51.						
52.						
53.						
54.						
55.						
56.						
57.						
58.						
59.						
60.						
61.						
62.						
63.						
64.						
65.						
66.						
67.						
68.						
69.						
70.						
71.						
72.						
73.						
74.						
75.						
76.						
77.						
78.						
79.						
80.						
81.						
82.						
83.						
84.						
85.						
86.						
87.						
88.						
89.						
90.						
91.						
92.						
93.						
94.						
95.						

D.1 Safety and Mission Assurance Plan Template (con't)

Safety and Mission Assurance Plan (SMAP)		
SMAP	Document No.: Document Number	Revision:
	Date: April 9, 2009	Page 18 of 18

Req ID	GLPR Section	Requirement Statement	Project Implementation Intent			
			Existing Project Doc/Section	Compliance		
				Full	Partial	None
96.						
97.						
98.						
99.						
100.						
101.						
102.						
103.						
104.						
105.						
106.						
107.						
108.						
109.						
110.						
111.						
112.						
113.						
114.						
115.						
116.						
117.						
118.						
119.						
120.						
121.						
122.						
123.						
124.						
125.						
126.						
127.						
128.						
129.						
130.						
131.						
132.						
133.						
134.						
135.						
136.						
137.						
138.						
139.						
140.						
141.						
142.						
143.						
144.						
145.						

D.2 Certificate of Flight Readiness

Project Certificate of Flight Readiness (CoFR)
Endorsement Signature Sheet

TITLE	NAME	SIGNATURE	DATE
Director, NASA Glenn Research Center		*N/A - Signature on certificate.*	
Deputy Director, NASA Glenn Research Center			
Director, Space Flight Systems Directorate*			
Director, Engineering Directorate			
Director, Safety and Mission Assurance Directorate			
Chief, Responsible SFSD Office			
Chief, Chief Engineer's Office			
GRC Project Manager*			
GRC Lead System Engineer			
GRC Safety and Mission Assurance Lead			

GRC 2062 (OCT 09) ***Also sign certificate.**

D.2 Certificate of Flight Readiness (con't)

GRC Certificate of Flight Readiness

At the _____ Review, the GRC Management Team has certified that the deliverable hardware requirements related to the GRC areas of responsibility have been satisfactorily completed. As of this Pre-Ship Review, there are no constraints related to the GRC areas of responsibility. The GRC hardware provided, including all supporting systems as applicable, are ready for hardware turnover, pending satisfactory closure of remaining tasks and issues identified in this Review and documented in the project's Open Work Closure Plan. The Open Work Closure Plan itemizes all remaining tasks and issues with their corresponding mitigation plan and closure criteria.

The GRC Management Team has certified:

(1) As-built configuration

(2) List of as-built parts, materials, and processes

(3) Status of all verification items with a list of open items and rationale for the items being open

(4) Listing, status, and remaining life of limited-life items

(5) Results of Acceptance Tests

(6) Status of all nonconformances, failures, and problem reports

(7) Waivers and deviations affecting flight acceptance, safety, and mission success

(8) Cleanliness certification

(9) Certification of flight software acceptance

_____	_____
Director, NASA Glenn Research Center	Date
_____	_____
Director, Space Flight Systems Directorate	Date
_____	_____
GRC Project Manager	Date

GRC 2062 (OCT 09) GLPR 7120.5.30 Appendix D.2

Appendix E. Internet Resources

NASA Online Directives Information System (NODIS) Library: http://nodis.hq.nasa.gov/

NASA Technical Standards Program: http://standards.nasa.gov/

Payload Safety: http://wwwsrqa.jsc.nasa.gov/pce/

Safety and Mission Assurance Requirements Tracking System (SMARTS):
http://pbma.hq.nasa.gov/

Safety & Mission Assurance Requirements Tree:
http://www.hq.nasa.gov/office/codeq/doctree/qdoc.htm

Electronic Document Management System (EDMS) (formerly Space Station Program Automated Library System or PALS):
http://iss-www.jsc.nasa.gov/ss/issapt/edms

Web sites with ELV User Guides:

Delta II and IV:
http://www.ulalaunch.com/index_products_services.html

Sea Launch:
http://www.sea-launch.com/customers_webpage/sluw

Atlas V:
http://www.ulalaunch.com/index_products_services.html

Pegasus:
http://www.orbital.com/NewsInfo/Publications/peg-user-guide.pdf

Taurus:
http://www.orbital.com/NewsInfo/Publications/taurus-user-guide.pdf

Minotaur:
http://www.orbital.com/NewsInfo/Publications/Minotaur_Guide.pdf