



**GLENN
PROCEDURAL
REQUIREMENTS**

Directive: GLPR 7120.5.30B
Effective Date: 12/07/2022
Expiration Date: 12/07/2027

COMPLIANCE IS MANDATORY

This Document Is Uncontrolled When Printed.
Validate prior to use at <https://nasa.sharepoint.com/sites/BMSLibrary>

Responsible Office: Code Q/Safety and Mission Assurance Directorate
Space Assurance Requirements (SAR)

TABLE OF CONTENTS

Preface

- P.1 Purpose
- P.2 Applicability
- P.3 Authority
- P.4 Applicable Documents and Forms
- P.5 Measurement/Verification
- P.6 Cancellation

Chapter 1. Responsibilities

- 1.1 GRC Management
- 1.2 Project Manager (PM)
- 1.3 Project Chief Engineer (PCE)
- 1.4 Lead Systems Engineer (LSE)
- 1.5 Chief Safety and Mission Assurance Officer (CSO)
- 1.6 Safety and Mission Assurance (S&MA) Lead
- 1.7 System Safety Lead Engineer
- 1.8 Reliability Lead Engineer
- 1.9 Quality Assurance (QA) Lead Engineer
- 1.10 Software Assurance (SA) Lead Engineer

Chapter 2.General Requirements

- 2.1 Description of General Requirements
- 2.2 Safety and Mission Assurance Plan (SMAP)
- 2.3 Use of Deviations
- 2.4 Use of Previously Designed, Fabricated or Flown Systems
- 2.5 Storage Requirements for Suspended Projects
- 2.6 Assurance Status Reports
- 2.7 Contractor Surveillance
- 2.8 GRC Assurance Review Requirements
- 2.9 Mishap Reporting and Investigation
- 2.10 Safety, Health, and Environmental

Chapter 3. Design and Verification

- 3.1 General Requirements
- 3.2 Overall Verification Program
- 3.3 Electrical Requirements and Verification
- 3.4 Structural and Mechanical Requirements
- 3.5 Electromagnetic Compatibility (EMC) Requirements
- 3.6 Radiation Requirements
- 3.7 Vacuum, Thermal, and Humidity Requirements
- 3.8 Flight System Performance Acceptance Test Requirements
- 3.9 Ground Support Equipment (GSE)

Chapter 4. System Safety

- 4.1 Introduction
- 4.2 System Safety Planning
- 4.3 Hazards Analysis
- 4.4 Failure Tolerance
- 4.5 Design for Minimum Risk and Similar Approaches
- 4.6 Internal GRC Review of Safety Products
- 4.7 Requirements Applicability

Chapter 5. EEE and Mechanical Parts Control

- 5.1 General Requirements
- 5.2 EEE Parts Selection and Screening
- 5.3 Mechanical Parts Selection and Screening
- 5.4 Procurement of Parts
- 5.5 Parts Storage Control
- 5.6 Storage Life Screening
- 5.7 Parts Identification List
- 5.8 Parts Risk Evaluation
- 5.9 Parts Subject to Metal Whisker Growth
- 5.10 Salvaged Parts

Chapter 6. Reliability, Availability, and Maintainability

- 6.1 General Requirements
- 6.2 RAM Requirement for an Integrated Process
- 6.3 RAM Management
- 6.4 RAM Plan
- 6.5 RAM Data
- 6.6 RAM Reports Archives
- 6.7 Reliability and Failure Tolerance
- 6.8 Variances from Two-Failure Tolerance Requirement
- 6.9 Probabilistic Risk Assessment (PRA)

Chapter 7. Quality Assurance (QA) Requirements

- 7.1 General Requirements
- 7.2 Quality Assurance Organization
- 7.3 Configuration Management (CM) and Verification
- 7.4 Identification and Traceability
- 7.5 Procurement and Contract Quality Assurance Requirements
- 7.6 Control of Fabrication Activities
- 7.7 Contamination Control
- 7.8 Electrostatic Discharge (ESD) Prevention

- 7.9 Nonconformance and Problem Reporting and Control
- 7.10 Alert Information
- 7.11 Inspection and Test of Stored Limited-Life Hardware
- 7.12 Metrology
- 7.13 Handling, Preservation, Marking, Packaging, Packing, and Transportation
- 7.14 Control of Government Property by Contractors
- 7.15 System Acceptance Review
- 7.16 Product Acceptance/Acceptance Data Package (ADP)
- 7.17 Control of Quality Records
- 7.18 Launch and Mission Initiation Operations

Chapter 8. Continuous Risk Management (RM)

- 8.1 Introduction
- 8.2 Risk Informed Decision Making (RIDM)
- 8.3 Continuous Risk Management (CRM)
- 8.4 General Requirements
- 8.5 Initial Risk Management Training
- 8.6 Implementation

Chapter 9. Flight Software Assurance and Software Safety (SASS)

- 9.1 SASS Procurement Planning
- 9.2 Responsibilities
- 9.3 Flight SASS Planning and Implementation

Chapter 10. Flight Programmable Logic Assurance

- 10.1 Flight Programmable Logic Assurance Procurement Planning
- 10.2 Responsibilities
- 10.3 Flight Programmable Logic Assurance Planning and Implementation

APPENDICES

- Appendix A . Definitions
- Appendix B . Acronyms
- Appendix C . Verification Matrix
- Appendix D . Templates and Forms
 - D.1 Safety and Mission Assurance Plan Template
 - D.2 Certificate of Flight Readiness
- Appendix E . Internet Resources

LIST OF FIGURES

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

LIST OF TABLES

- Table 2-1—Control Plans
- Table 3.4-1—Executive Summary of NASA-STD-7001 Rev A Verification Test Requirements³
- Table 3.4-2—Component Minimum Workmanship Random Vibration Test Levels
- Table 3.4-3—Example of Weight Contingencies Applied at the Component and Subsystem Level.

Change History

Distribution: BMS Library

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.
- 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 NPR 7120.5 programs and projects, NPR 7120.8 projects if project management makes the decision to follow this document, 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 to 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 6 development and demonstration articles. 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.
- h. This directive is applicable to documents developed or revised after the effective date of this GLPR.
- i. In this directive, all mandatory actions (i.e., requirements) are denoted by statements

containing the term “*shall*.” The term “*may*” denotes a discretionary privilege or permission, “*can*” denotes statements of possibility or capability, “*should*” denotes a good practice and is recommended, but not required, “*will*” denotes expected outcome, and “*are/is*” denotes descriptive material.

- j. In this directive, all document citations are assumed to be the latest version, unless otherwise noted.

P.3 Authority

- a. NASA Policy Directive (NPD) 8700.1, NASA Policy for Safety and Mission Success
- b. NASA Procedural Requirements (NPR) 7120.5, NASA Space Flight Program/Project Management Requirements

P.4 Applicable Documents and Forms

- a. FAR Part 46, Quality Assurance
- b. NASA FAR Supplement (NFS) Part 1846, Quality Assurance
- c. NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy
- d. NPR 1441.1, NASA Records Retention Schedules
- e. NPR 7120.5, NASA Space Flight Program and Project Requirements
- f. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements
- g. NPR 7123.1, NASA Systems Engineering Processes and Requirements
- h. NPR 7150.2, NASA Software Engineering Requirements
- i. NPR 8000.4, Risk Management Procedural Requirements
- j. NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping
- k. NPR 8705.2, Human-Rating Requirements for Space Systems
- l. NPR 8705.4, Risk Classification for NASA Payloads
- m. NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
- n. NPR 8715.3, NASA General Safety Program Requirements
- o. NPR 8715.7, Expendable Launch Vehicle Payload Safety Program
- p. NPR 8735.1, Exchange of Problem Data Using NASA Advisories and the Government-Industry Data Exchange Program (GIDEP)
- q. NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects
- r. GLPR 1280.1, Glenn Research Center Quality Manual
- s. GLPR 7120.5.20, GRC Project Deviation/Waiver Process
- t. GLPR 7123.35, GRC Project Technical Review Procedure
- u. GLPR 8000.4, GRC Procedural Requirements for Risk Management

- v. GLPR 8730.6, Control of Inspection, Measuring, and Test Equipment.
- x. GLPR 8739.1, Glenn Procedural Requirements: Software Assurance
- y. GLHB-QER-8730.1, Electric, Electronic, Electromechanical (EEE) and Mechanical Parts Management
- z. GLP-Q-1280.2, Corrective and Preventive Action
- aa. GLP-QEA-8735.2, Requirements for Establishing Government Mandatory Inspection Points
- bb. GLP-QER-8730.4, Electrical, Electronic, and Electromagnetical (EEE) Parts Assurance
- cc. GLWI-Q-8700.3, Safety and Mission Assurance Engineering Review Board (SERB)
- dd. NASA-HDBK-4008, Programmable Logic Devices (PLD) Handbook
- ee. NASA-STD-4003, Electrical Bonding for NASA Launch Vehicles, Spacecraft, Payloads, and Flight Equipment
- ff. NASA-STD-4005, Low Earth Orbit Spacecraft Charging Design Standard
- gg. NASA-STD-5001, Structural Design and Test Factors of Safety for Space-Flight Hardware
- hh. NASA-STD-5002, Load Analyses of Spacecraft and Payloads
- jj. NASA-STD-5005, Standard for the Design and Fabrication of Ground Support Equipment
- jj. NASA-STD-5017, Design and Development Requirements for Mechanisms
- kk. NASA-STD-5019, Fracture Control Requirements for Spaceflight Hardware
- ll. NASA-STD-6008, NASA Fastener Procurement, Receiving Inspection, and Storage Practices for Spaceflight Hardware
- mm. NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft
- nn. NASA-STD-7001, Payload Vibroacoustic Test Criteria
- oo. NASA-STD-7002, Payload Test Requirements
- pp. NASA-STD-7003, Pyroshock Test Criteria
- qq. NASA-STD-8739.1, Workmanship Standard for Polymeric Application on Electronic Assemblies
- rr. NASA-STD-8739.4, Crimping, Interconnecting Cables, Harnesses, and Wiring
- ss. NASA-STD-8739.5, Workmanship Standard for Fiber Optic Terminations, Cable Assemblies, and Installation
- tt. NASA-STD-8739.6, Implementation Requirements for NASA Workmanship Standards
- uu. NASA-STD-8739.8, NASA Software Assurance and Software Safety Standard
- vv. NASA-STD-8739.14, NASA Fastener Procurement, Receiving Inspection, and Storage Practices
- ww. AFSPCMAN 91-710, Launch Vehicles, Payloads, and Ground Support Systems Requirements
- xx. ANSI/AIAA S-080, Space Systems-Metallic Pressure Vessels, Pressurized Structures, and Pressure Components
- yy. ANSI/AIAA S-081, Space Systems-Composite Overwrapped Pressure Vessels (COPV)
- zz. 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)

- aaa. ASME Y14.5, Dimensioning and Tolerancing
- bbb. Centre Spatial Guyanais (CSG)-RS-10A-CN, Safety Regulations Volume 1
- ccc. CSG-RS-21A-CN, Centre Spatial Guyanais Safety Regulations Volume 2–Part 1.
- ddd. CSG-RS-22A-CN, Centre Spatial Guyanais Safety Regulations Volume 2–Part2
- eee. EEE-INST-002, Instructions for EEE Parts Selection, Screening, Qualification, and Derating
- fff. IPC J-STD-001, Requirements for Soldered Electrical and Electronic Assemblies
- ggg. IPC J-STD-001S, Space Applications Electronic Hardware Addendum to IPCJ-STD-001, Requirements for Soldered Electrical and Electronic Assemblies
- hhh. JAXA Management Requirement (JMR)-002, Launch Vehicle Payload Safety Standard
- iii. JSX 2001015, H-II Transfer Vehicle (HTV) Cargo Safety Requirements
- jjj. JSX 2008041, HTV Cargo Safety Review Process
- kkk. JSX 2009059, HTV Cargo Safety Certification Process for Disposal
- lll. Kennedy Space Center Procedural Requirements (KNPR) 8715.3, NASA KSC Payload & Cargo Ground Safety Requirements
- mmm. Military Standard (MIL-STD)-461E, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
- nnn. Multi-Purpose Crew Vehicle (MPCV) 70038, MPCV Program Hazard Analyses Requirements
- ooo. NASA Parts Selection List (NPSL)
- ppp. PT-TE-1415, Power System Corona Testing
- qqq. P32928-103, Requirements for International Partner Cargo Transported on Russian Progress and Soyuz Vehicles
- rrr. P32958-106, Technical Requirements for Hardware to be Stored or Operated on the ISS Russian Segment
- sss. SAE AS9100, Quality Management Systems- Requirements for Aviation, Space and Defense Organizations
- ttt. Space Launch System (SLS)-RQMT-015, SLS Program Hazard Analysis Requirements
- uuu. SMC-S-016, Test Requirements for Launch, Upper Stage, and Space Vehicles
- vvv. Space Station Program (SSP) 30599, Payload Safety Review and Data Submittal Requirements
- www. SSP 50021, Safety Requirements Document for International Space Station
- xxx. SSP 50146, Safety Review Process
- yyy. SSP 50808, ISS to Commercial Orbital transportation Services Interface Requirements
- zzz. SSP 50835, Common Interface Requirements Documents
- aaaa. SSP 51721, ISS Safety Requirements Document

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 shall be removed from this document. Eventually, when all engineering requirements have been removed, this document shall only contain safety and mission assurance requirements.

P.5 Measurement/Verification

- a. The GRC Program and Project Assurance Division (PPAD) conducts annual assessments of programs/projects to verify compliance with this document. Compliance is 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 (CAPA) in accordance with GLP-Q-1280.2 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 1280.1.

P.6 Cancellation

This GLPR cancels GLPR 7120.5.30, Space Assurance Requirements w/Change 3 (03/08/2022), dated March 4, 2016.

LAURENCE SIVIC *Digitally signed by LAURENCE SIVIC*
Date: 2022.12.07 15:23:02 -05'00'

Laurence A. Sivic
Associate Director

Distribution: BMS Library

Chapter 1. Responsibilities

1.1 GRC Management *shall*:

- a. Assign program/project manager (PM) and program/project chief engineer (PCE) (or for smaller projects a Project Lead Engineer) and program/project chief safety and mission assurance officer (CSO) (or for smaller projects a Project S&MA Lead) to the program/project.
- b. Ensure the technical integrity of the project through participation in reviews of program/project and technical plans.
- c. Assist the program/project team with obtaining the institution capabilities necessary to plan and implement the program/project.

1.2 Project Manager (PM) *shall*:

- a. Ensure all safety and mission assurance requirements are satisfactorily accomplished.
- b. Ensure the development, approval, and maintenance of the project safety and mission assurance plan.

1.3 Project Chief Engineer (PCE) *shall*:

Serve 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. Smaller projects may have a Project Lead Engineer assigned in place of the PCE.

1.4 Lead Systems Engineer (LSE) *shall*:

Lead 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) *shall*:

- a. Serve as the program/project-level safety and mission assurance (S&MA) technical authority, and ensures that the program/project and technical planning is consistent with Agency and Center S&MA design processes, specifications, rules, best practices, etc., necessary to fulfill mission performance requirements for the project.
- b. Assist the PM in ensuring the S&MA requirements are satisfactorily accomplished and have direct access to project management.
- c. For program/project and technical planning:
 - (1) Leads the development of the program/project S&MA 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 S&MA plan component to the Systems Engineering Management Plan.

1.6 Safety and Mission Assurance (S&MA) Lead *shall*:

- a. For projects that do not warrant a CSO, the S&MA lead serves as the project-level safety and mission assurance point of contact and ensures that the project and technical planning is consistent with Agency and Center S&MA design processes, specifications, rules, best practices, etc., necessary to fulfill mission performance requirements for the project.
- b. Assist the PM in ensuring the S&MA requirements are satisfactorily accomplished and have direct access to project management.
- c. Specifically, for program/project and technical planning, the S&MA lead:
 - (1) Leads the development of the program/project S&MA 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.
 - (6) Provides the S&MA plan component to the Systems Engineering Management Plan.

1.7 System Safety Lead Engineer *shall*:

- a. Assure 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. Assure the development of a System Safety Technical Plan (SSTP) during the project formulation phase and update the plan throughout the system life cycle
- c. Ensure that system safety models are constructed to support the implementation of the risk-informed decision framework.
- d. Ensure 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.
- e. Establish the methods and tools that are used in the risk-informed framework.
- f. Check and validate the methods and tools before implementation and obtain concurrence from the PM.
- g. Document the basis for the methods and tools used and analytical results.

1.8 Reliability Lead Engineer *shall*:

- a. Assure 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. Ensure that reliability and maintainability (R&M) activities (addressing hardware, software, firmware, human elements, and interactions between them) are planned and implemented.
- c. Ensure 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.
- d. Ensure 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.

1.9 Quality Assurance (QA) Lead Engineer *shall*:

- a. Assure 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. Ensure program planning and acquisition documents incorporate applicable requirements of this document, including specification of applicable quality system requirements.
- c. Assure applicable QA requirements flow 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.
- d. Identify safety/mission critical attributes and associated government mandatory inspection points.
- e. Ensure 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 *shall*:

- a. Assure 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. Work 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.
- c. Assure that the programmable logic device (PLD) 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.
- d. Work with the program/project to review, analyze, advise, and report on the PLD development process. In addition, they report all mission-critical and safety-critical findings to the OSMA, as well as program, and/or project management.

Chapter 2. General Requirements

2.1 Description of General Requirements

2.1.1 The GRC PM has primary responsibility for ensuring assurance requirements are satisfactorily accomplished. However, the CSO and/or S&MA lead *shall* assist the PM in this effort and has direct access to developer management.

2.1.2 The S&MA program *shall* operate concurrently with all other elements.

2.1.3 The project is required to plan, implement, and organize an S&MA 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 S&MA 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.

2.1.4 The S&MA program *shall* apply to all work accomplished by the project including contractors, subcontractors, and suppliers. The development may be in-house or by an outside contractor.

2.1.5 The requirements of this document were originally intended for Space Shuttle missions. Iterations have brought in additional requirements, including ISS payloads and Gateway. As various Agency, commercial and international standards and requirements may be applicable to specific projects, the PM, PCE/PLE and CSO/S&MA lead will work together to assure the intent of this requirements set is met by other requirements levied on the project. The Project Safety and Mission Assurance Plan (SMAP) *shall* go through a Safety and Mission Assurance Engineering Review Board (SERB) prior to release. Once released, the SMAP is the projects S&MA requirements set. Projects of higher risk posture (e.g., Class D-, “Do No Harm”, commercial payloads) will follow the same process where the PM and S&MA lead will jointly determine the appropriate requirements commensurate with the project’s risk posture, and then present the SMAP to a SERB for Code Q review and authorization.

2.1.6 Code Q/Safety and Mission Assurance Directorate, and Code L/Research and Engineering Directorate are responsible for requirements in this document. Code Q and Code L are jointly responsible for content in Chapters 1 and 2. Code L is responsible for content within Chapter 3 and Code Q is responsible for all remaining chapters. Code L is the Technical Authority over chapter 3 content, with Code Q being the Technical Authority over all other requirements in this document. The approval authority for requirement deviations and waivers, or questions on interpretation, will be addressed by the Responsible Office(s) for the associated chapter. Code L is responsible for verification and validation tracking of all chapter 3 requirements. This is usually accomplished through an engineering requirement’s tracking document.

2.2 Safety and Mission Assurance Plan (SMAP)

2.2.1 The S&MA support, dictated by the CSO, *shall* be implemented with an approved SMAP, which addresses all sections of this SAR directive.

2.2.2 The SMAP *shall*:

- a. Document how the program/project is going to meet the requirements within this directive.
- b. Include SAR reference paragraphs, deliverables, and performing organizations.

- c. Identify any noncompliance to the requirements in the SAR and provide justification in the SMAP.
- d. Require verification to SAR requirements 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.
- e. Be reviewed by the PM, PCE/PLE and CSO/S&MA lead. Approval will be per the GRC QE Safety and Mission Assurance Engineering Review Board (SERB) process.
- f. Assure any proposed changes to the approved SMAP are submitted to the PM and CSO for approval prior to implementation. Projects are encouraged to make maximum use of their own existing procedures.
- g. Require procedures referenced in an approved SMAP are available for information at the developer's facility.

2.2.3 The approval signatures certify that the SMAP implements all NASA GRC's applicable institutional requirements or that the authority responsible for those requirements has agreed to the modification of those requirements in the SMAP.

2.2.4 For an outside contract, the contractor's SMAP *shall*:

- a. Be delivered by the date specified in the contract.
- b. Be delivered with the associated contractor's practices and procedures referenced in the SMAP.
- c. Not take precedence over the SAR. If inconsistencies between the contractor's approved SMAP and the SAR become evident during the contract period of performance, clarification and/or any possible contract changes will need to be processed through the procurement official.
- d. Require any new procedure or any proposed changes to the approved procedures be submitted to the PM, PCE/PLE and CSO/S&MA lead, as appropriate, for review and/or approval in accordance with the contract.

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

Table 2-1—Control Plans

Description	Paragraph
Safety and Mission Assurance Plan	2.2
Storage Plan	2.5
Mishap Preparedness and Contingency Plan	2.9
Verification Plan	3.2
Fracture Control Plan	3.4.1
Structural Verification Plan	3.4.1
Mass Property Plan	3.4.1
Materials and Processes Control Plan	3.4.7.1
Systems Safety Technical Plan	4.2
EEE Parts Control Plan	5.2.1

Mechanical Parts Control Plan	5.3.3
Reliability, Availability, Maintainability Plan	6.4
Probabilistic Risk Assessment Plan	6.9.1.2
Quality Assurance Plan	7.1.4
Configuration Management Plan	7.3.3
QA Surveillance Plan	7.5.13.1
Fastener Integrity Plan	7.6.3.12
Contamination Control Plan	7.7.1
Risk Management Plan	8.4.3
Software Assurance Plan	9.3.2
Programmable Logic Device Configuration Management Plan	10.3.1.2

2.3 Use of Deviations

Deviations *shall* be:

- a. Written for each SAR requirement that the program/project does not meet.
- b. Submitted to the PM, PCE/PLE and the CSO/S&MA lead for review.
- c. Stored in an appendix in the SMAP.
- d. Used per GLPR 7120.5.20, GRC Deviation/Waiver Process, to document and approve agreements affecting specific requirements that intentionally release a project from meeting that requirement.

2.4 Use of Previously Designed, Fabricated, or Flown Systems

When a system that was designed, fabricated, or flown previously is to be used, the developer is required to evaluate how the system complies with the S&MA requirements in this document, and document risks of noncompliance. 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.

- a. At a minimum, a verification readiness review *shall* be conducted for any reflights to address the reverification and test program.
- b. Programs and projects should have plans in place to decommission the hardware at mission completion.

2.5 Storage Requirements for Suspended Projects

2.5.1 Suspended programs/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.

2.5.2 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.

2.5.3 The storage plan *shall* include, but is not limited to:

- a. A detailed list of the hardware, software, and documents being stored.
- b. The status of the flight system going into storage, including completed verification activities, outstanding problem reports, and waivers/deviations.
- c. The configuration for storage, including the appropriate drawings and procedures to be followed to go from flight configuration to storage configuration and back.
- d. 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).
- e. Operational limits during storage (to ensure sufficient life remains for the mission).
- f. Handling and storage requirements, including safety precautions, temperature, and humidity.
- g. Attributes of the storage area(s), including environmental controls, accessibility controls (i.e., bonded storage), and requirements for periodic QA monitoring.
- h. Plans for temporary archiving of project data and records (if needed) and for maintaining configuration control of all items stored.
- i. 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).
- j. Identification of project risks and mitigation strategies once the hardware comes out of storage.
- k. The version of flight and ground support equipment (GSE) software (executables and source code) and how stored.
- l. Identification of the software configuration management system and how this system is implemented (local server, Web based, etc.).
- m. Identification and use of software development tools that are required to run the flight and/or ground software (e.g., compilers).

2.5.4 All project records *shall* be maintained per NPR 1441.1.

2.5.5 The storage area environment and accessibility *shall* be:

- a. Controlled, as needed, to prevent damage, deterioration, or loss of the items stored.
- b. Checked periodically to verify controls are functioning properly and stored items continue to be well maintained.

2.6 Assurance Status Reports

2.6.1 The program/project CSO/S&MA lead *shall* provide status reports to S&MA management in accordance with the S&MA management reporting schedule.

2.6.2 The reports *shall* cover items such as those listed below as well as those discussed in the individual sections of this document:

- a. Key S&MA organization and personnel changes.
- b. Significant S&MA risks.
- c. Safety and deviation/waiver issues.
- d. Status of S&MA activities in manufacturing, testing, and operations.
- e. Supplier and subcontract S&MA activities.
- f. Audit, nonconformance, and problem reports.
- g. Review status.
- h. Parts list, parts problems, and ALERT findings.
- i. Performance and problem trend analyses.

2.7 Contractor Surveillance

2.7.1 The GRC projects *shall*:

- a. 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.
- b. Delegate responsibilities and authority to other government agencies in a letter of delegation, in accordance with NPR 8735.2C, Chapter 8, Protocols and Requirements for Delegating Quality Assurance Contract Administration functions to the Defense Contract Management Agency (DCMA). Or with an independent assurance contractor with a GRC contract.

2.7.2 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 per NPR 8735.2.

2.7.3 The contractor, upon request, *shall* provide:

- a. The S&MA documents, records, and equipment required to perform these activities to government representatives.
- b. Government representatives with an acceptable work area within its facilities when requested.

2.8 GRC Assurance Review Requirements

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

2.9 Mishap Reporting and Investigation

The project *shall*:

- a. Develop a Mishap Preparedness and Contingency Plan consistent with the requirements of NPR 8621.1.

- b. Use the NASA Mishap Information System for documenting any reportable mishaps.
- c. Make initial notification within 24 hours of the mishap.

2.10 Safety, Health, and Environmental

The Glenn Safety and Health Management System and Environmental Management System apply to all activities, operations, and organizations at GRC, both Lewis Field and Armstrong Test Facility. 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-FE-8500.1).

Chapter 3. Design and Verification

3.1 General Requirements

3.1.1 The design of a system being developed by a program/project is driven by requirements from a number of sources. Requirements development is performed in accordance with sections 2.2, 2.3 and 2.4 of GLPR 7123.2, Systems Engineering for Flight and Ground Systems.

3.1.2 The program/project plans and implements a verification program, in accordance with section 2.8 of GLPR 7123.2 to ensure that all design requirements (program/science, safety, assurance, interface, and operational) for the system being developed are satisfied. System assurance requirements that are to be verified are defined in this section and throughout the rest of this document.

3.1.3 The program/project will determine which integration requirements documents (e.g., interface control documents) need to be followed. These documents provide the basis for the integration testing that it is required in these areas. Payload integration with the experiment carrier (e.g., Expedite the Process of Experiments to Space Station (EXPRESS) pallet) as described in this section is worked directly with the integration centers. Integration of the payload/carrier with the launch vehicle is the responsibility of the integration center with support from the payload developer.

3.1.4 Payloads *shall* meet NASA-STD-7002.

3.1.5 The following Lessons Learned *shall* be reviewed for the project. The project team (PM engineering and S&MA) will agree on any implementation of these lessons learned and will document the path forward with rationale in the SAR compliance matrix.

a. Flight hardware test sequencing should occur in the following order:

- (1) Sinusoidal or transient vibration, random vibration, pyroshock, and acoustics, as required. The order among these dynamics tests may be interchanged.
- (2) Thermal-vacuum Thermal Cycle and Ambient Pressure Thermal Cycle testing.

Note: Rationale for dynamic testing can induce defects that are not always detected during the test but show up afterward in thermal testing. Reversing the order may result in induced test defects not getting detected until flight – see <https://llis.nasa.gov/lesson/779>.

b. Vibration, acoustics, and pyroshock testing should supply power to electronic assemblies and monitor the electrical functions continuously during testing. (Rationale: Intermittencies in electronic circuitry can often be detected during vibration but may not be observed under ambient functional testing see <https://llis.nasa.gov/lesson/784> and <https://llis.nasa.gov/lesson/780>)

3.2 Overall Verification Program

3.2.1 A verification program begins with the development of a verification plan that is based on the outcome of the requirements development process which identifies the program/project verification requirements, defines the method(s) of verification, provides traceability to

original requirements, and defines the requirement applicability to systems. It concludes when the required verifications are completed (compliant or approved nonconformance) as outlined in the plan.

3.2.2 The methods of verification include analytical investigations, inspections (including physical property measurements), demonstrations, tests, or a combination of these. Tests include simulating the environments to be encountered. These environments may include handling and transportation, prelaunch, launch, on-orbit, retrieval, reentry, and landing.

3.2.3 The verification plan is initiated following the systems definition review or requirements definition review, as defined in the program/project Systems Engineering Management Plan (SEMP) and be consistent with NPR 7123.1. For GRC inhouse projects, implementation will be in accordance with GLPR 7123.2. The implementation should be consistent with the assembly levels at which design requirements are written (e.g. component, subsystem, system), and should be outlined in the verification plan.

3.2.4 Any unique characteristics that drive the design and verification of the system *shall* be identified at the Preliminary Design Review (PDR) and communicated to the program/project team so risk mitigations can be tracked in a timely and effective manner as detailed in Chapter 9.

3.2.5 Flight systems will undergo acceptance testing in accordance with the program/project verification plan.

3.2.6 Prototype or protoflight systems will undergo qualification to demonstrate compliance with the requirements outlined in the verification plan. When hardware is planned to be reflowed, 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.

3.2.7 The verification plan, developed in accordance with GLPR 7123.2, should contain the following information often in a verification matrix format:

- a. Requirements Document-identify the source document from which the verification element was obtained.
- b. Paragraph Reference-identify the paragraph from the source document.
- c. Requirement Title-specify the specific requirement in a brief descriptive form.
- d. Methods of Verification-identify methods of verification.
- e. Verification Approach Summary-define the activities through which the verification should be accomplished.
- f. Closure Requirement-specify how closure will be accomplished and documented.
- g. Safety Closure Reference-clearly identifies those related to safety closure (e.g. verification of hazard report controls).
- h. The verification matrix, as well as the verification plan, will be updated throughout the program/project to reflect the latest documentation and status changes.

3.3 Electrical Requirements and Verification

The system *shall* comply with:

a. IPC-2221, Generic Standard on Printed Board Design

Note: IPC-2221 establishes standards for the design and manufacture of Printed Wiring Boards (PWB). The document defines acceptable clearances, substrates, adhesives, through holes, component placement, impedance controls, etc. This document also points to additional documents with requirements for rigid PWBs, flexible PWBs, multichip modules, parallel communication PWBs, and high density interconnects, at least one of which will always be applicable and required.

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

Note: The purpose of NASA-STD-4003 is to define the basic electrical bonding requirements for NASA launch vehicles, spacecraft, payloads, and equipment. Its intent is to provide fundamental aerospace electrical bonding requirements, as well as to classify electrical bonds according to their purpose. These requirements aim to minimize electrical potential difference across all equipment, ensuring proper operation.

c. NASA-STD-4002, Mitigating In-Space Charging Effects.

Note: When electrical systems are operated in a space environment they can accumulate charge unintentionally. If not mitigated, this charge can cause errors and damage electronics. This handbook applies to all mission environments including Medium Earth Orbit (MEO), Low Earth Orbit (LEO), Geosynchronous Earth Orbit (GEO), Polar Earth Orbit (PEO)), as well as spacecraft in other energetic plasma environments such as those at Jupiter and Saturn, and interplanetary solar wind charging environments.

d. NASA-STD-4005, Low Earth Orbit Spacecraft Charging Design Standard, if the system could be exposed to electrical potentials greater than 55 Volts **and** operates in an orbit with a perigee below 2000 km mean sea level.

Note 1: When high voltage systems are operated in the Earth ionosphere, it can cause the spacecraft to accumulate charge unintentionally. If not mitigated, this charge can cause errors and damage electronics. Unlike NASA-STD-4002, this standard is specifically targeted for missions in LEO orbit.

Note 2: The program/project should use NASA-HDBK-4006, Low Earth Orbit Spacecraft Charging Design Handbook, as additional design guidance and theoretical background for meeting requirements found in NASA-STD-4005.

Note 3: If the system contains “high voltage” electrical potentials the program/project should use NASA-HDBK-4007, Spacecraft High-Voltage Paschen and Corona Design Handbook, for guidance in understanding how to mitigate breakdown and discharge resulting from the operation of high-voltage systems in space.

Note 4: The term “high voltage” in this conditional is defined as the potential, above which, electrical breakdown phenomena are likely to occur. This is intentionally

ambiguous as the absolute potential for a breakdown event is dependent on many parameters including frequency, magnitude, geometry, environment, and cannot be explicitly stated for all cases. Breakdown voltages can range from tens of volts in microwave systems to thousands of volts in utility systems. NASA-HDBK-4007 provides guidance on the risk of breakdown and can be used to determine if an application is at risk of electrical breakdown phenomena.

- e. AIAA S-111A-2014, Qualification and Quality Requirements for Space Solar Cells, if the system uses Solar Cells
- f. AIAA S-112A-2013, Qualification and Quality Requirements for Electrical Components on Space Solar Panels, if the system uses Solar Panels

3.4 Structural and Mechanical Requirements

3.4.1 General Requirements

The verification plan *shall*:

- a. Include a structural verification plan, fastener integrity plan, and mass properties control plan.
- b. Include a fracture control plan if the verification plan is for program/projects that are part of a human spaceflight system, as well as payloads or experiments operated on crewed vehicles.
- c. List the structural and mechanical requirements and their origin.
- d. State the method of verification (analysis, test, demonstration 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, on-orbit operation, and crew handling.

3.4.2 Safety-Critical and Fracture-Critical Structures

3.4.2.1 Safety-Critical: 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*:

- a. Show positive margins of safety for structural elements.
- b. Show structural containment against penetration for containment devices.

3.4.2.2 Fracture-Critical: The SCS may include a subset of components whose failure would present catastrophic hazards, that is, they are under one of the following classifications: (1) low-released mass, (2) fail-safe, contained, (3) Non-Hazardous Leak Before Burst (NHLBB), (4) low risk parts, etc. (see Section 3.4.5). These components are termed “fracture critical” and *shall*:

- a. Be shown through analysis, inspection, and/or test to be safe from failure throughout the mission.

- b. For human spaceflight systems, as well as payloads or experiments operated on crewed vehicles, have life predictions, quality control and traceability, and in-depth inspection criteria detailed in a Fracture Control Plan developed and implemented by the hardware developer

3.4.2.3 The program/project should obtain a user's handbook that defines the interfaces and environments for which the payload should be designed, and the carrier-specific structural verification requirements.

3.4.2.4 While the concepts of safety-critical and fracture-critical structures are intended to address mission safety, the hardware developer should also address the functional integrity of the hardware (Mission Assurance).

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

3.4.3 Structural Loads

3.4.3.1 The 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.

3.4.3.2 Flight hardware *shall* be designed to maintain structural integrity during all phases of the expected life cycle. Verification of the hardware to the structural load environments requires a combination of test and analysis.

- a. Structural loads consideration for flight structures and systems *includes* static and dynamic loads encountered during assembly, testing, transportation, launch, ascent, space operations, extraterrestrial operations, descent, and landing.
- b. Hardware is generally exposed to the following four 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, (3) high-frequency (31- to 10,000- Hz) acoustic excitation, and (4) high frequency (100hz - 10,000+Hz) shock excitation.

3.4.3.3 Estimation of loads for the payload is an iterative process throughout the life cycle of the hardware until launch. 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; however, if payload is class D per NPR 8705.4, there is provision to tailor (Section 4.3.6 of NASA-STD-7001).

3.4.3.4 Limit load is the maximum anticipated load experienced by a structure during its design service life. 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.

3.4.4 Factors of Safety

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. The NASA-STD-5001 establishes design and test factors, as well as service life factors, to be used for space flight hardware development and verification.

3.4.5 Margins of Safety

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

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

i.

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

3.4.5.3 The NASA-STD-5020 or the NASA-TM-106943 (based on National Space Transportation System (NSTS) 08307) is a detailed guide for performing bolted joint analysis.

3.4.5.4 The determination of MS for a payload is normally a labor-intensive process. Typically, a Finite Element Model (FEM), is generated. This model is exercised for all load cases, and the resulting member loads and/or stresses are determined. These member loads and/or stresses are used in hand calculations to determine MS for the credible failure modes. The MS *shall*:

- a. Be well documented in a stress report.
- b. Be updated for the as-built condition or any redesign of the hardware.
- c. Include the FEM model and the static test used to verify unless a “no test” approach has been approved.

3.4.5.5 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.

3.4.5.6 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 are 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. Verifications *shall*:

- a. Assure hand-calculations of MS that utilize Finite Element Analysis outputs such as member and joint loads are performed.
- b. Assure an experienced engineer, from the same discipline and one who understands the methodologies performs the formal checking and signs 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.

3.4.5.7 Reviewing, on the other hand, is done at a higher level and lower fidelity than checking. A reviewer *shall* 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.

3.4.6 Fracture Control

3.4.6.1 All human spaceflight systems, as well as payloads or experiments operated on crewed vehicles *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-HDBK-5010 provides guidelines and examples as a supplementary document to the NASA-STD-5019 for fracture control implementation.

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

- a. 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.
- b. Fracture Control Plan. The program/project *shall*:
 - (1) 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.
 - (2) Ensure payload-specific fracture control plans are approved by the fracture control authority.
- c. Fracture Classification. All space flight hardware parts *shall* 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. Nonfracture critical hardware includes:

low-released mass, fail-safe, contained, NHLBB, low risk parts, etc. For composite materials, the term crack also includes delaminating, defects due to manufacturing, impact damage, and in-service damage.

- d. Damage Tolerant Analysis or Test. The life of all fracture-critical parts is 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, and *shall*:
 - (1) Show parts resist failure due to the presence of cracks during the entire service life multiplied by the required service-life factor.
 - (2) Show the service-life factor for all NASA space flight hardware that is part of human spaceflight systems, as well as payloads or experiments operated on crewed vehicles is four or greater.
- e. 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.
- f. Nondestructive Evaluation (NDE). All fracture-critical parts *shall* be subjected to NDE or proof testing to screen for internal and external cracks.

g. Fracture Control Summary Report

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

3.4.6.3 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.

3.4.7 Materials and Processes Selection, Implementation and Control Requirements

3.4.7.1 Programs/projects *shall* be compliant to NASA-STD-6016 for materials and process selection, implementation and control for 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.

Note: Programs, projects and elements are responsible for contractually levying these requirements down through every tier of hardware development, to the lowest component-level suppliers. These requirements provide a common framework for materials and processes control practices on all NASA programs/projects.

3.4.7.2 For in-house projects, projects *shall* follow Glenn Level Procedure (GLP) GLP-LMA-8072.1, Materials and Processes for Spaceflight Hardware, to establish a standard methodology for meeting NASA-STD-6016 at NASA Glenn Research Center (GRC).

Note: This GLP describes M&P deliverables that are expected and provides a description of typical roles and responsibilities needed for effective implementation of NASA-STD-6016. GLP-LMA-8072.1 does not replace NASA-STD-6016, nor does it serve as the project M&P Plan which is required by NASA-STD-6016.

3.4.8 Pressurized Systems

3.4.8.1 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 3.4.6).

3.4.8.2 Pressurized systems that are part of human spaceflight systems, as well as payloads or experiments operated on crewed vehicles *shall*:

- a. Be two-failure tolerant regarding pressure; that is, maximum design pressure will not be exceeded with any combination of two credible failures.
- b. Meet the requirements of ANSI/AIAA S-080, Space Systems-Metallic Pressure Vessels, Pressurized Structures, Pressure Components, or ANSI/AIAA S-081, Space Systems-Composite Overwrapped Pressure Vessels, depending on the type of vessel. A new COPV design that is linerless is being developed. An associated standard is under development.
- c. Comply with NASA-STD-7012, Leak Test Requirements.

3.4.9 Strength Testing

3.4.9.1 Structural designs of space flight systems *shall* 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.

3.4.9.2 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.

3.4.9.3 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).

3.4.9.4 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.

3.4.10.2 Component Random Vibration Testing

3.4.10.2.1 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).

3.4.10.2.2 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.

- a. If appropriate, as specified in Section 3.4.10.3, these test levels will also envelope the component minimum workmanship levels.
- b. For application of force limiting, see NASA HDBK-7004, Force Limited Vibration Testing.

3.4.10.3 Workmanship

3.4.10.3.1 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 Grms

3.4.10.3.2 The minimum workmanship random vibration test specification *shall* be imposed on electrical, electronic, and electromechanical components weighing 50 kg (110 lb) or less. The minimum spectrum for a component whose mass exceeds 50 kg (110 lb) should be evaluated on an individual basis. A methodology for deriving a minimum workmanship vibration specification for components larger than 50 kg (110 lb) is given in Appendix B.1.3 of NASA-STD-7001b. When the minimum workmanship test level exceeds the qualification/flight acceptance/ protoflight levels, the minimum random vibration test level *shall* be the greater of the workmanship or protoflight levels across the entire 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 to the International Space Station (ISS).

3.4.10.3.3 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.

3.4.10.4 Stowed Components

3.4.10.4.1 Hardware designed and launched in a stowed condition *shall*:

- a. Have the qualification/protoflight hardware tested in the stowed configuration. 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.
- b. Expose electrical, electronic, and electromechanical components weighing 50 kg (110 lb) or less to workmanship levels via either testing in the stowed or hard-mounted configuration. If hardware is greater than 110lb it must be evaluated on a case-by-case basis as discussed in NASA-STD-7001. 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.
- c. Only screen to the vibration levels seen in the stowed configuration test (which is likely to be below the 6.8 G_{rms} workmanship level), highly vibration-sensitive flight/protoflight hardware.

3.4.10.4.2 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.

3.4.10.4.3 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.

3.4.10.5 Retesting of Reflight Hardware

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).

3.4.10.6 Additional Vibroacoustic Testing

3.4.10.6.1 The need to perform vibroacoustic testing at the subsystem level *shall* be assessed, 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.

3.4.10.6.2 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.

3.4.10.6.3 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.

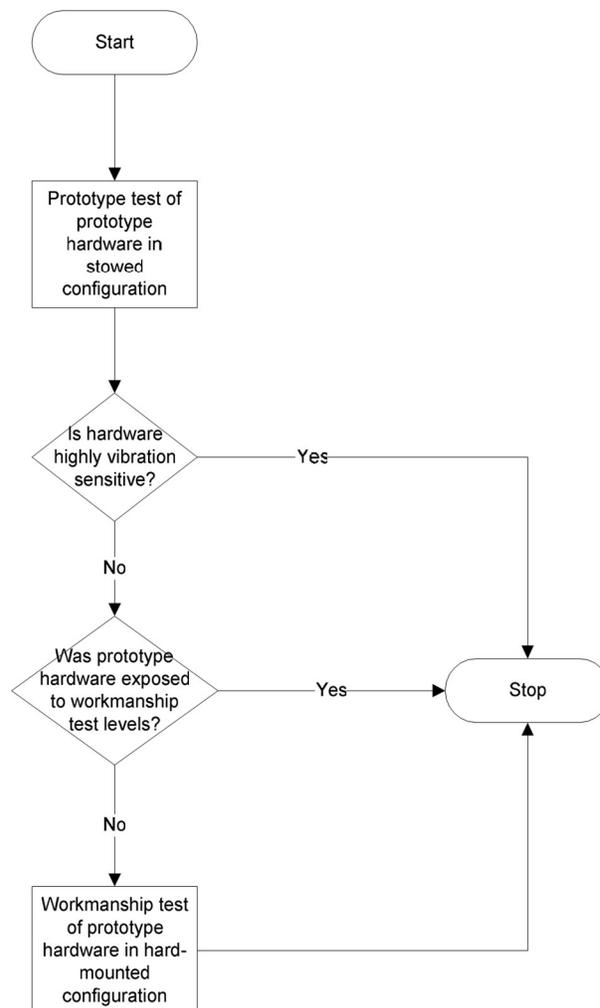


Figure 3.4-1—Vibration Testing of Stowed Hardware for Protoflight Project.

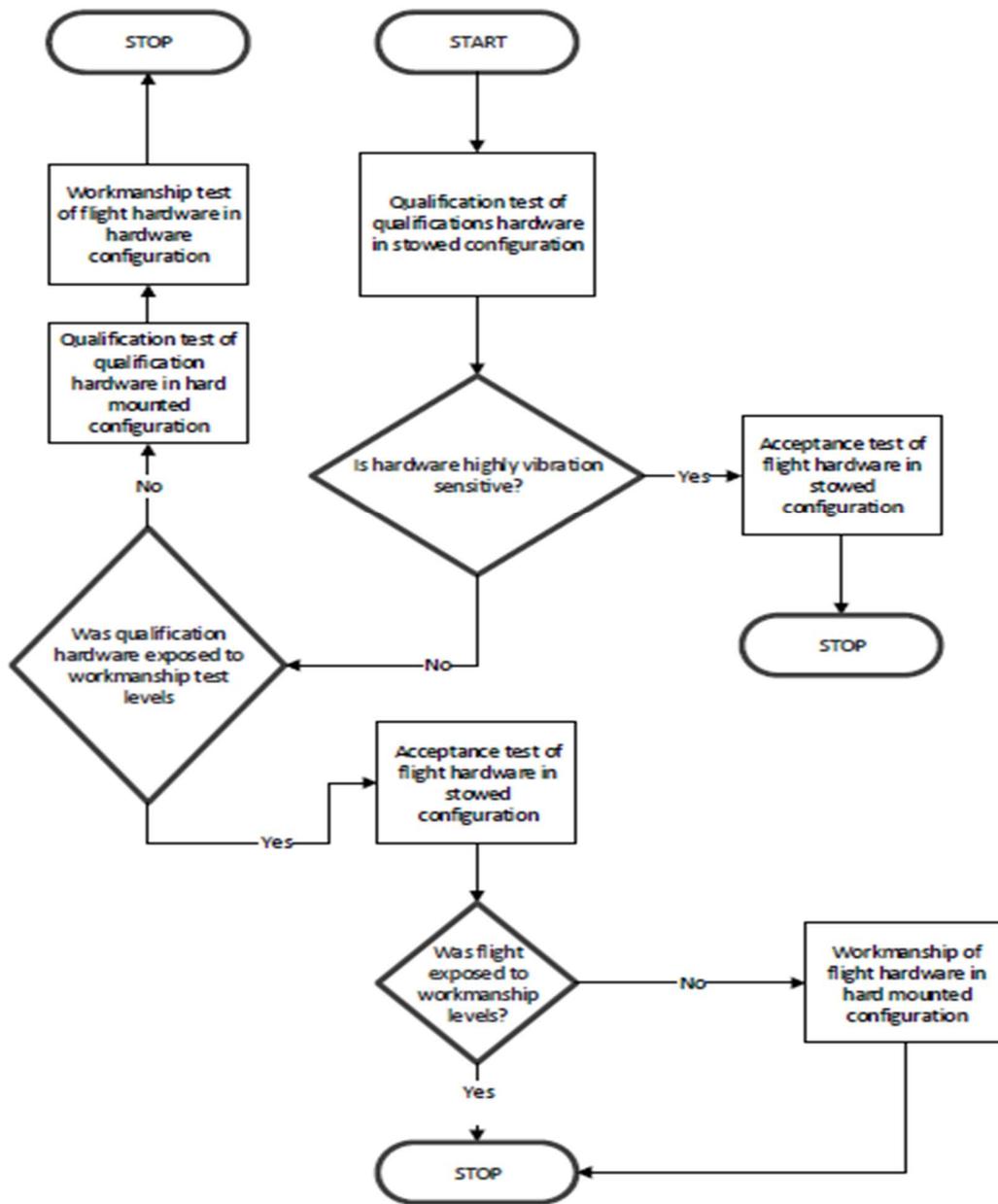


Figure 3.4-2 Vibration Testing of Stowed Hardware for Prototype Project

3.4.11 Shock (Mechanical and Pyro)

3.4.11.1 General

3.4.11.1.1 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.

3.4.11.1.2 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.

3.4.11.1.3 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.

3.4.11.1.4 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.

3.4.11.1.5 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.)

3.4.11.2 Flight Acceptance

3.4.11.2.1 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.

3.4.11.2.2 An end-to-end test of any pyrotechnic device *shall* be conducted for demonstration of acceptance for flight.

3.4.12 Mechanical Function

To meet the requirements of NASA-STD-5017, mechanisms *shall*:

- a. Complete kinematics analysis of all mechanical operations.
- b. Show by analysis 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.
- c. 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.

3.4.12.1 Qualification Testing

3.4.12.1.1 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.

3.4.12.1.2 High- and low-energy tests *shall* also be conducted to prove positive margins of strength and function.

3.4.12.1.3 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.

3.4.12.1.4 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.

3.4.12.1.5 As a minimum, however, successful operation at temperature extremes 10°C beyond the range of expected flight temperatures *shall* be demonstrated.

3.4.12.2 Flight Acceptance Testing

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 7.2.

3.4.13 Pressure Profile

3.4.13.1 The need for a pressure profile test *shall* be assessed for all subsystems.

3.4.13.2 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.

3.4.13.3 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.

3.4.13.4 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.

3.4.14 Mass Properties

3.4.14.1 Component and system mass properties are required as input to loads definition and strength analysis activities throughout the hardware development cycle. Mass is a critical attribute of space flight hardware and needs to be budgeted and tracked throughout the life of the program/project. To assure proper mass budgeting, the project *shall*:

- a. Define a project weight budget early in the conceptual design phase to guide the design effort.
- b. Verify as-built mass properties by test before delivery of hardware for flight. The International Society of Allied Weight Engineers can be a source of information on verification test methods.

3.4.14.2 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.

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

- a. Identified (or Basic) Mass Properties. 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.
- b. Weight Growth Allowance (or Contingency). 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/project *shall*:
 - (1) 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 latter approach is used, the subsystem contingencies may be rolled up using the RSS method if approved by the customer and the payload integrator.
 - (2) Define and justify the weight contingencies to be applied throughout the program/project.
- c. Predicted (or Current) Mass Properties. The predicted mass properties of an item are the identified mass properties plus the weight growth allowance.
 - (1) The predicted mass properties are the mass properties that *shall* be compared to the budgeted mass properties.

(2) Worst-case mass properties *shall* 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.

- d. 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 *shall* 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.]

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

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

3.5 Electromagnetic Compatibility (EMC) Requirements

3.5.1 EMC Requirements

3.5.1.1 Relative to EMC, flight hardware *shall*:

- a. 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.
- b. 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.

3.5.1.2 Flight hardware *shall* meet the appropriate version of MIL-STD-461, Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, as specified and tailored by the carrier.

3.5.1.3 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.

3.5.2 EMC Guidance

3.5.2.1 The purpose of the EMC is to ensure that equipment are operated correctly in the expected 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 *shall* be considered to achieve EMC; emissions and susceptibility.

3.5.2.2 Emission issues are related to the unwanted generation of electromagnetic energy by various sources. Countermeasures are taken to reduce such generation and the propagation 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 expected electromagnetic disturbances.

3.5.2.3 The EMC requirements are developed by programs and projects specific to their needs. This assures adequate margin for the payload's susceptibility to the surrounding environment's conduction and radiation interference. In addition, it also takes into account of the effect of the payload's emission to the equipment surrounding it.

3.5.2.4 The EMC control plans are used to manage the process of achieving EMC through the control of EMI. EMC Control Plans *shall*:

- a. Assure the power distribution system, control functions, signal, data processing, and distribution functions are managed through attention to circuit board layout, electrical isolation, grounding, filtering, and shielding.
- b. Assure EMI is controlled in the time domain (in-rush current at turn on and turn off, digital rise/fall times) and in the frequency domain (signal pass bands, cable lengths, motors, and switching power supplies).

3.5.2.5 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 *shall*:

- a. Address how risks for noncompliant COTS components are addresses.
- b. Be managed at the integrated system level
- c. Be able to achieve EMC.

3.5.2.6 Below are some design issues with COTS equipment:

- a. 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 *shall* be provided no later than PDR. 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.
- b. 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, electromagnetic gaskets, screened apparatus, and metal compartments within equipment. Shielding is normally applied to wiring connecting individual equipment or to reduce cable-to-cable coupling in signal circuits.

- c. 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

3.6.1 Programs and projects defined as Category 1 or 2, and/or Class A, B or C payloads *shall* determine the applicable ionizing radiation environment via available data, documentation, research and analyses. Program and project category are determined by NPR 7120.5. Payload class is determined by NPR 8705.4.

3.6.2 The program/project *shall* create a risk mitigation plan to address potential effects of operating in the applicable environment determined in 3.6.1. Ionizing radiation effects include single event effects (SEE) such as single event upset, single event burnout, single event transient, and single event gate rupture, as well as total ionizing dose effects such as semiconductor lattice displacement damage.

3.6.3 The program/project *shall* conduct parts testing and/or analysis to verify that the space flight system will operate as intended in the applicable environment determined in 3.6.1.

3.7 Vacuum, Thermal, and Humidity Requirements

Vacuum (if applicable), thermal, and humidity tests *shall*:

- a. 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, and space vehicle), storage, and pre and post launch conditions on the carrier.
- b. Act as an environmental screening to stimulate latent defects that can cause infant mortality.

3.7.1 Worst-Case Predicted Temperature Range

3.7.1.1 The worst-case predicted temperature range (WPTR) *shall* be established for all credible combinations of worst-case cold and hot conditions that could occur during a mission. These temperatures are to be ascertained during the design process by development of analytical thermal models based on mission profiles taking into account the exterior boundary conditions and interior sources of thermal energy. Examples of variables to consider include power dissipation, material property changes (beginning and end-of-life), and orbit and vehicle orientations.

3.7.1.2 Hardware Design Temperature Range *shall*:

- a. For payload electronics (except detectors and instrument-unique hardware) be designed to operate within +71 to –34 °C or WPTR extended by ± 21 °C, whichever is more severe. This

temperature range is defined within SMC-S-016, "Test Requirements for Launch, Upper Stage, and Space Vehicles."

- b. For Protoflight units use limits of +71 to -34 °C or WPTR extended by ±16 °C, whichever is more severe.
- c. For Spacecraft structures and other non-electronic units be designed to qualification or protoflight temperatures as defined SMC-S-016, Test Requirements for Launch, Upper Stage, and Space Vehicles.
- d. Use the appropriate design factors of safety over the qualification and protoflight temperature range.

3.7.2 Validation of Thermal Properties

All thermal analyses *shall* employ thermal properties validated to be accurate for materials and mission flight parameters over the life cycle of the mission.

3.7.3 Compliance with Requirements

The developer *shall*:

- a. Demonstrate compliance by conducting a set of tests and analyses that collectively meet the above requirements
- b. 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.
- c. The test and analysis plan *shall* be included as part of the review process, and the initial document reviewed no later than PDR.

3.7.4 Testing Levels

Test temperature range, margins, number-of-cycles, and humidity tests *shall* be determined using guidance provided in SMC-S-016, Test Requirements for Launch, Upper-Stage, and Space Vehicles.

3.7.5 Description of Applicable Testing

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. Determination of which components, units, or systems are subjected to the tests described in this section *shall* be accomplished using the guidance provided in SMC-S-016.

3.7.5.1 Thermal Cycling

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. Thermal cycling *shall*:

- a. Assure complete specification performance testing is performed at the temperature extremes on the first and last hot and cold cycles and at ambient temperature prior to and following thermal cycling.

- b. Be operated at least in its nominal functioning mode for the remaining cycles. The system under test does not need to be operated at hot and cold survival temperatures.
- c. Operate failure free for the final four consecutive cycles.

3.7.5.1.1 Ambient Pressure Thermal Cycle

Systems under test *shall*:

- a. If designed/required to operate in vacuum or in microgravity environments not having forced convection, be subjected to the requirements of Section 3.7.5.1.2, Thermal Vacuum.
- b. For systems other than listed in 3.7.5.1.1 above, 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.

3.7.5.1.2 Thermal Vacuum

Thermal-vacuum tests *shall*:

- a. Only be 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.

Note: If thermal-vacuum testing is performed, thermal cycle testing should still be performed to stimulate latent problems and help expose workmanship issues. Thermal cycle temperature extremes will be chosen to validate hardware workmanship and should be chosen to not excessively stress components. However, the temperature rate of change and number of cycles will be severe enough to stress components with the intent to identify latent defects. The thermal-vacuum test plan will take into account parts used, criticality of the function and project risk posture. S&MA will be included in discussions regarding the testing and limits.

- b. Assure thermal cycles are conducted at a vacuum level of 1.33×10^{-3} Pa (1×10^{-5} torr) or lower.
- c. Assure supplemental heating and cooling support systems (such as cold plates and chillers) are used when necessary to condition the system under test.

3.7.5.2 Thermal Balance Testing

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*:

- a. Be verified under simulated on orbit 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.
- b. Have thermal balance tests conducted at a vacuum level of 1.33×10^{-3} Pa (1×10^{-5} torr) or lower.

3.7.5.3 Humidity

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.

3.7.6 Description of Applicable Analysis

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*:

- a. 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. Be completed and available no later than PDR.

3.8 Flight System Performance Acceptance Test Requirements

3.8.1 Burn-In Tests

3.8.1.1 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 system level operation should be demonstrated. 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. Failed and replaced parts in the system can have component level burn-in tests to avoid putting additional time on the entire system. The approach for failed parts requires concurrence from safety and engineering technical authorities.

3.8.1.2 The project *shall* develop a screening and qualification plan for safety critical components controlling critical hazards according to EEE-INST-002, Instructions for EEE Parts Selection, Screening, Qualification, and Derating.

3.8.1.3 Burn-in for safety critical parts *shall* precede thermal vacuum testing (reference MSFC-HDBK-670).

3.8.2 Mission Simulation Test

3.8.2.1 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.

3.8.2.2 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

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 should be addressed in the Integration Plans and Agreements.

3.9 Ground Support Equipment (GSE)

All GSE *shall* meet the following:

- a. NASA-STD-5005 requirements
- b. KNPR 8715.3, “KSC Safety Practices Procedural Requirements” for ISS payloads.
- c. GLP-Q-8715.1 when used at the GRC
- d. The engineering technical authority for a project, along with the SMA technical authority, will explicitly define what items are required to be defined as GSE deliverables, and any tailoring of NASA-STD 5005.

Note: GSE is the ground HW/SW that interfaces with flight hardware in its final configuration. Not everything that touches flight hardware should or needs to be classified as GSE. Intermediate items used during the development and assembly of flight hardware do not generally rise to the level of the GSE designation. For typical GRC science payloads, the GSE rules would only apply after subassemblies become the complete payload. Application of the standard should be tailored commensurate to the risk associated with failure of the flight hardware just prior to or during operational use. Projects may apply GSE requirements over and above the intended use, although this can add significant cost and effort. Designation of GSE should be weighed against hazards and the project risk posture.

- e. Loads imparted to flight hardware during transportation and handling are no more than 80 percent of the design flight loads.

Note: 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.

Chapter 4. System Safety

4.1 Introduction

4.1.1 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.

4.1.2 This section is intended to flow down requirements from NPR 8715.3, and NPR 8705.2 when appropriate, for system safety applicable to space programs or space projects managed by GRC.

4.2 System Safety Planning

4.2.1 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 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/or 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.

4.2.2 System Safety Assurance Reviews are conducted in conjunction with other program/project milestones. The purpose of these reviews is to evaluate the status of system safety and risk analyses, risk management, verification techniques, technical safety requirements, and program/project implementation throughout all the phases of the system lifecycle.

4.2.3 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, the ISS payloads.

4.2.4 The approach used to comply with the system safety requirements *shall* be an:

- a. Agenda item at each of the program/project reviews listed above and system safety requirements
- b. Integral part of all technical developments.

4.3 Hazards Analysis

4.3.1 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, Fault Tree Analysis (FTA), System Hazard Analysis, Subsystem Hazard Analysis, Functional Hazard Analysis, Operating and Support Hazard Analysis, Software Hazard Analysis, and Integrated Hazard Analysis. 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.

4.3.2 The following is the order of precedence of methods/strategies that *shall* be used to mitigate hazards:

- a. Eliminate the hazard.
- b. 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.
- c. Provide caution and warning devices.
- d. Develop and implement special procedures including the use of personnel protective equipment.

4.3.3 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

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 4.7, Implementation of Failure Tolerance, does not alleviate the need to prevent failures.

4.5 Design for Minimum Risk and Similar Approaches

4.5.1 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 *shall* be well understood and verifiable. Examples of DFMR solutions include applying factors of safety for primary structures, 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.

4.5.2 Some programs may utilize other approaches such as demonstrating compliance to certain design and construction standards, and instead document via exemption packages failures tolerance

alternatives. Those alternate rationales and engineering evidence *shall* be documented and verifiable. Those requirements are also listed in Section 4.7.

4.6 Internal GRC Review of Safety Products

All GRC developed or sponsored safety products, for example, Safety Data Packages (SDP) and System Safety Analysis Reports, *shall* undergo an internal independent assessment prior to external center release. If the product is developed in-house, the review will follow the S&MA SDP SERB process. If the product is developed by an outside contractor/service provider, the product will be reviewed and approved/concurred by the SMAD.

4.7 Requirements Applicability

The following table provides the applicable process and technical safety requirements documents for each type of flight system being developed. Additional safety requirements documents may be referenced within these top-level documents. Payloads flown on an expendable launch vehicle (ELV), international partner vehicle, or commercial carrier vehicle to the ISS for operations there will also meet the ISS payload safety requirements.

Table 4.7 –Applicable Process and Technical Safety Requirements Documents

Hardware Classification	Governing Safety Document(s)
Orion and Space Launch Systems	MPCV 70038, SLS-RQMT-015
ISS Payload (includes Development Test Objective payloads)	SSP 30599, SSP 51721, KNPR 8715.3
ISS Vehicle	SSP 30599, SSP 51721, SSP 50808
Payload Safety Program (<i>formerly titled Expendable Launch Vehicle</i>)	NPR 8715.7
Progress and Soyuz Payloads	SSP 50146, P32928-103, P32958-106
Ariane Payload	CSG-RS-10A-CN, CSG-RS-21A-CN, CSG-RS- 22A-CN
Japanese H-IIA Payload	JMR-002, JSX 2008041, JSX 2009059, JSX2001015
US Ground Support Equipment and Ground Operations Systems	KNPR 8715.3, RMS-002
Air Force Space Command (AFSPC) ranges, including Eastern Range and Western Range	AFSPCMAN 91-710
Commercial Carrier (Dragon, Cygnus) Payload	SSP 50835, SSP 50808
Gateway, Gateway Payloads Launch Services Program	GP 10024, TBD, NPR 8715.7, NASA-STD-9719.24

Chapter 5. EEE and Mechanical Parts Control

5.1 General Requirements

The requirements outlined in this section are in accordance with the general guidelines in NASA-STD 8739.10 and apply to all flight system fidelities including qualification and protoflight systems. Programs/projects *shall*:

- a. Plan and implement an EEE, and mechanical parts control program.
- b. Allocate resources for the use of the NASA Electronic Parts Applications Reporting and Tracking System by the electronics design teams.
- c. Select and control parts based on performance, environmental (ground and flight), criticality for safety and mission success, and lifetime requirements.

5.2 EEE Parts Selection and Screening

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

The EEE parts control plan *shall*:

- a. Be identified in the SMAP. This plan can be either a standalone document or part of the SMAP. The EEE Parts Control Plan may be tailorable to the project risk classification. Class D or CubeSat projects may not require the complete set of EEE Parts Assurance requirements.
- b. Be established to verify that the electrical form, fit, and function of EEE Parts meet program or program/project requirements.
- c. Contain a section to describe the approach for avoiding, detecting, dispositioning, controlling, and reporting counterfeit EEE parts.
- d. 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, parts obsolete and any other requirements necessary to meet mission objectives.

Note: Additional guidance in developing the EEE parts control plan can be found in GLHB-QER-8730.1 and GLP-QER-8730.4.

5.2.2 EEE Parts Selection and Grade

The grade level of a given EEE 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. The EEE parts control plan *shall*:

- a. Specify the grade level of parts to be selected:
 - (1) Parts will be chosen based on the risk (low, medium, high, or unknown) as described in the EEE Parts Risk Assessment Matrix (GLHB-QER-8730.1).
 - (2) If commercial and/or industrial parts are chosen, the risk is unknown and parts will be assessed on a case- by-case basis. Commercial and industrial parts are usually of higher risk than qualified military or high-reliability parts.
- b. Have a standard (or preferred) parts list for programs/projects based on the level of parts chosen:
 - (1) Parts to be used in flight hardware will be selected from the standard parts list.
 - (2) Parts not on the standard parts list will be considered nonstandard
 - (3) Nonstandard parts will require review and approval before use in flight hardware.
- c. The NASA Parts Selection List (NPSL) and EEE-INST-002 has been developed to serve as a parts selection tool for NASA space flight programs. In general, parts listed in the NPSL and EEE-INST-002 have established procurement specifications, have available source(s) of supply, can meet a wide range of application needs, and have been assessed for quality, reliability, and risk. Parts listed in the NPSL and EEE-INST-002 *shall*:
 - (1) Be considered for inclusion in standard parts list, and
 - (2) Be considered for inclusion in standard or preferred parts lists.

5.2.3 Flight EEE Parts Qualification

The EEE parts selected for flight hardware *shall* be:

- a. Qualified to verify that materials, design, performance, and long-term reliability of the parts are consistent with the specifications and intended applications.
- a. From manufacturers listed on the qualified parts list or qualified manufacturers list for the specification for parts procured to military specifications.
- b. Qualified per an approved source control drawing, the qualification methods of EEE-INST-002, or an approved qualification plan for nonmilitary parts.
- c. Qualified for the specified grade level, specifically parts used in an application requiring a higher grade level.

5.2.4 Flight EEE Parts Screening

The EEE parts screening serves to identify and remove any nonconforming parts from an otherwise acceptable lot of parts or to reject unacceptable lots. The screening of EEE parts used in flight hardware *shall*:

- a. Be done for all flight EEE parts. Additional requirements for parts in high reliability applications include:
 - (1) Screening at the piece part level
 - (2) Following the requirements of the appropriate military or NASA specification, an approved source control drawing, or an approved screening plan.

- b. Require additional screening when a part of higher or unknown risk is used in an application requiring lower risk parts. Requirements for additional screening can be found in EEE-INST-002 and must be met. The developer may adopt their own upgrade screening requirements with GRC approval.
- c. Be reviewed on a case-by-case basis for low budget projects, which are typically shorter in duration (0 to 14 days) but exclude man-rated launch vehicles. In such projects, screening at the piece part level is not required. 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.
- d. Be made practical for commercial off-the-shelf (COTS) assemblies and assessed at a higher level (assembly or system level) versus at a piece part level. Required screening tests at the assembly or system level can be found in the COTS section of GLHB-QER-8730.1 and include:
 - (1) Burn-In
 - (2) Thermal Cycle
 - (3) Vibration

5.2.5 Derating

The derating of parts improves the reliability of systems (reference Preferred Reliability Practice PD-ED-1201). All EEE parts (including cables and wires) *shall* be used in accordance with the de-rating requirements and guidelines of EEE-INST-002. Another NASA de-rating document, such as MSFC-STD-3012, 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

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-QER-8730.6 (See also: JSC-67551, Avionics Ionizing Radiation Effects Standards).

5.2.6.1 Total Ionizing Dose

5.2.6.1.1 Parts *shall* be selected 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.

5.2.6.1.2 The expected total dose *shall* be defined for each mission.

5.2.6.1.3 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).

5.2.6.2 Single Event Effects (SEE)

5.2.6.2.1 Parts *shall* be selected so that equipment meets specified performance requirements

when exposed to the SEE radiation environment. The SEE includes single event upsets, transients, latch-ups, burnouts, gate ruptures, and snapbacks.

5.2.6.2.2 Safety-critical circuits *shall* be designed so that they will not fail because of SEE or are capable of recovery if SEE occurs.

5.2.6.2.3 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*:

- a. Demonstrate through testing (see Sections 3.6.) or analysis whether the selected parts can withstand SEE.
- b. Compare the parts list to the NASA Electronics Parts and Packaging Program radiation data for EEE part types. Preference to selection of radiation hardened or radiation tolerant parts, as well as appropriate circuit design and parts de-rating, are combined practices to mitigate the impact of SEEs.

5.2.6.3 Displacement Damage

5.2.6.3.1 Parts *shall* be selected 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.

5.2.6.3.2 Evaluation of susceptibility to displacement damage *shall* be through testing or analysis.

5.2.7 Corona and Arcing

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 3.7.5.1.2 and reference MSFC-STD-531, Preferred Reliability Practices PD-ED-1202 and PT-TE-1415.)

5.2.8 Inspection Prior to Assembly

5.2.8.1 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.

5.2.8.2 The EEE parts that are safety or mission critical *shall* be tested to verify and certify their electrical performance prior to pre-launch processing of flight systems or subsystems. This testing may have to be performed at the circuit card or sub-assembly level depending upon technical or configuration constraints.

5.3 Mechanical Parts Selection and Screening

5.3.1 Mechanical parts *shall* be selected to meet program/project reliability and availability requirements over mission life.

5.3.2 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 parts and vendors that were previously qualified and meet space flight performance, environmental, criticality, and life cycle requirements.

5.3.3 Mechanical Parts Control Plan

5.3.3.1 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.

5.3.3.2 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.

5.3.3.3 Fastener control *shall* address lot testing for structural strength and material composition and storage and use control.

5.3.3.4 Program, project, and Government Furnished Equipment (GFE) managers *shall* implement NASA-STD-8739.14 for control of fasteners.

5.3.4 Inspection Prior to Assembly

5.3.4.1 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.

5.3.4.2 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) as part of a qualification model unit prior to the assembly into flight systems or subsystems.

5.4 Procurement of Parts

5.4.1 General Requirements

5.4.1.1 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. Detailed guidance for the control of counterfeit parts is provided in SAE AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition.

5.4.1.2 Procurements *shall*:

- a. Clearly identify the specification for items being purchased (2) Require certification of conformance to the required specifications. (3) Show traceability to the original manufacturer for parts purchased from authorized or franchised distributors (4) Be coordinated among programs and centers whenever feasible.
- b. Be screened for Government-Industry Data Exchange Program (GIDEP) notices and NASA Advisory impacts through the NASA Advisories, Notices and Alerts Distribution and Response Tracking system (NANADARTS) per Section 8.10.(6) Utilize available surveys and audits to determine whether suppliers meet program or project requirements.

5.4.1.2 The results of surveys, audits, product inspections, qualification testing and other activities performed by GRC and other NASA Centers, other Government agencies, accredited third- party organizations, or the private sector may be used to verify the capability and qualification of parts suppliers. The results of surveys and audits performed by GRC *shall* be provided to other NASA Centers via the NASA Supplier Assessment System.

5.4.2 Parts Obsolescence and Diminishing Manufacturing Sources

To assure parts availability for the duration of the project the project shall:

- a. Review parts selection and procurement to ensure parts availability for repair and new builds throughout the projected life of the equipment.
- b. Not select parts that are inactive for new design.
- c. Evaluate the project life cycles and mission life to determine if mission success could be negatively impacted by parts obsolescence.
- d. describe a process for monitoring parts procurement for obsolescence and mitigating the effects of parts obsolescence in the EEE Parts Control Plan.

5.5 Parts Storage Control

Bonded storage requirements for all parts are covered in Section 7.6.4.

5.6 Storage Life Screening

5.6.1 As some types of parts may fail or drift while in storage, parts assemblies *shall* be subjected to functional retest or recalibration prior to flight.

5.6.2 The program/project verification plan *shall* contain the details of the calibration sensitive items and their required calibration cycle.

5.6.3 If there is any system modification because of a failure during the acceptance test, the functional acceptance test *shall* be repeated.

5.6.4 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

5.7.1 A Parts Identification List (PIL) for EEE and mechanical parts *shall*:

- a. Be prepared, maintained, and updated by the program/project in accordance with the program/project's configuration control system.
- b. Be submitted to the GRC project as a project deliverable if a contract project, or to the GRC project CM for retention in a computer-readable form.
- c. Be reviewed against GIDEP Failure Experience Data and NASA Parts Advisories (see Section 7.10).
- d. Include as a minimum the following information: part number, part name or description, original manufacturer name or Commercial and Government Entity number, quantity, drawing number, and name of the next higher assembly where part is located.

Note: The part number is the number to which the part is procured, which is the military specification part number if it is a military part, a source control drawing part number if it is manufactured to the requirements of such a drawing, or the manufacturer's part number.

5.7.2 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.

5.7.3 The program/project *shall* maintain traceability by part number; original manufacturer, screening serial number, and lot date code for all parts assembled into flight hardware (see Section 8.4).

5.7.4 For COTS electronics, mechanical parts, electromechanical hardware or hardware such as circuit cards, sub-assemblies, cables or other products, traceability *shall* be maintained by serial number, original manufacturer, and model number.

5.8 Parts Risk Evaluation

5.8.1 The risk associated with each part *shall* be evaluated according to Section 5.2.1 and 5.3.3 and based on program/project requirements.

5.8.2 Lower risk and/or backup components (sparing) *shall* be used to meet the program/project availability goal.

5.8.3 The risks involved with using parts with medium, high, or unknown risks shall be defined through program/project data, analyses, or tests; unknown risks must also capture concerns and uncertainties associated with its use and application from project management, project engineering and project S&MA...

5.9 Parts Subject to Metal Whisker Growth

Program, project, and GFE managers *shall* mitigate risks associated with lead-free solder and surface finishes in accordance with criteria provided in the NASA-STD-8739.10.

5.10 Salvaged Parts

5.10.1 The selection and use of salvaged, reclaimed, or recycled parts *shall* be supported by objective quality evidence attesting to compliance with technical attributes specified in the parts' configuration baseline.

5.10.2 Technical rationale *shall* describe how such parts are to be verified to meet program or project requirements. Selection of parts for which objective quality evidence is not available, that do not meet configuration baseline technical requirements, or whose availability may have been compromised due to previous use are dispositioned as a waiver in accordance with Section 8.9.2.

Chapter 6. Reliability, Availability, and Maintainability

Note: 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.

6.1 General Requirements

6.1.1 The program/project along with Safety and Mission Assurance *shall* collaborate in order to identify the requirements, activities and resources needed to assure that system design meets the required level of RAM.

6.1.2 The RAM disciplines *shall* verify through analysis and review of testing or documentation that the system design meets RAM requirements. The following table summarizes some of the RAM requirements for space programs/projects.

Table 6.1 - RAM Requirements Summary Table for Space Programs/Projects

Requirements	Method of Verification
<p>System RAM Design Performance Requirements</p> <p>Qualitative</p> <ul style="list-style-type: none"> • 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 <p>Quantitative</p> <ul style="list-style-type: none"> • System Reliability • Subsystem (or Functional) Reliability Allocation) • Expected Operating and Storage Life 	<p>Qualitative</p> <ul style="list-style-type: none"> • Failure Modes & Effects Analysis (FMEA) • Failure Modes, Effects, and Criticality Analysis (FMECA) • Critical Items List (CIL) and Retention Rationale • Fault Tree Analysis (FTA) • System Functional Flow Block Diagrams • Single Point Failure (SPF) list with Risk Mitigation <p>Quantitative</p> <ul style="list-style-type: none"> • Reliability Allocation • Reliability Modeling and Analysis • Fault Tree Analysis (FTA) • Limited Life Items List and Plan
<p>System RAM Design Performance Requirements</p> <p>Qualitative</p> <ul style="list-style-type: none"> • System Survival and Intended Mission Environment <p>Quantitative</p> <ul style="list-style-type: none"> • Maintainability and Availability Allocations. Examples are: <ul style="list-style-type: none"> - 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 	<p>Qualitative</p> <ul style="list-style-type: none"> • Environmental Stress Screening <p>Quantitative</p> <ul style="list-style-type: none"> • Maintenance Task Analysis • Maintainability Analysis • Operational Availability analysis
<ul style="list-style-type: none"> • System Maintenance Concept 	<ul style="list-style-type: none"> • Maintainability Concept Document • Corrective and Preventive Maintenance Plans
<ul style="list-style-type: none"> • RAM Engineering Tasks 	<ul style="list-style-type: none"> • RAM Program Plan
<ul style="list-style-type: none"> • Assessment 	<ul style="list-style-type: none"> • Progress Toward Achieving RAM Requirements at Milestone Reviews • Identification of Areas of Improvement in RAM Reporting
<ul style="list-style-type: none"> • Integration of RAM Processes 	<p>Business Management System (BMS) Work Instructions for RAM processes</p> <p>Include a Flow of Information and Review Between RAM Engineering, and S&MA Disciplines</p>

6.2 RAM Requirement for an Integrated Process

6.2.1 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.

6.2.2 All disciplines *shall* provide information, data, and participation with RAM engineering to plan, establish, document, and implement a RAM program.

6.2.3 The RAM program *shall* encompass the following areas:

- a. System RAM design and operational performance requirements (qualitative and quantitative).
- b. System maintenance concepts.
- c. Requirements and tasks for RAM engineering and analysis.
- d. Review of testing.
- e. Software, firmware, PLD, and human-induced faults.
- f. Assessment of progress toward achieving RAM requirements and identification of areas for improvement.

6.2.4 The program/project systems engineering and components engineering groups *shall*:

- a. Participate in qualitative analyses, such as Failure Modes and Effects Analysis (FMEA) and Failure Modes, Effects, and Criticality Analysis (FMECA), and quantitative RAM requirements and analysis by addressing design areas where RAM improvement is needed.
- b. Providing information required to update RAM models and analyses
- c. Responding to the Critical Items List (CIL), derived from the FMEA by designing single point failures or providing data and other information required to develop retention rationale.
- d. Participating in the development of the CIL and its retention rationale.
- e. Supporting the process over the course of the program or project.

6.3 RAM Management

6.3.1 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.

6.3.2 The PMs and S&MA *shall* manage the RAM program.

6.3.3 The RAM engineering *shall* be tracked for progress against each major milestone goal.

6.3.4 At major milestone reviews, progress toward achieving the reliability requirements, including identification of areas for improvement *shall* be provided.

6.4 RAM Plan

6.4.1 The PMs and the SR&QA managers *shall* ensure that a RAM plan is prepared and tailored

in order to apply to a specific program or project.

6.4.2 The RAM Plan (which can be included as part of the SMAP) *shall* address the requirements specified in this document for RAM.

6.4.3 The RAM effort for each program/project *shall* be governed by the plan that will be contained in the program or project's 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.

6.5 RAM Data

The PMs *shall* provide and maintain RAM data from test, prelaunch, flight, and recovery for use as heritage data. The Center S&MA functional manager is responsible for usage of RAM data in RAM analyses.

6.6 RAM Reports Archives

6.6.1 The program/project's configuration management system *shall* maintain an archive of all RAM reports developed for the program or project.

6.6.2 The Program and Project Assurance Division will keep a file of all RAM reports developed for programs/projects.

6.7 Reliability and Failure Tolerance

6.7.1 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). Reliability is verified by reliability analysis using accepted modeling techniques and data in which uncertainties are incorporated.

6.7.2 Where this cannot be accomplished with a specified confidence level, the design of safety critical operations/functions *shall* have failure tolerance and safety margins in which critical operability and functionality are ensured.

6.7.3 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:

- a. Safety-critical systems will be designed to have failure tolerance and safety margins.
- b. Safety-critical systems will be designed so that no combination of two failures and/or operator errors will result in loss of life (fail-safe as a minimum).
- c. No single failure or operator error will result in system loss/damage or personnel injury.
- d. System design will provide functional redundancy in those cases where there is insufficient time for recovery or system restoration.

Note: For human space systems, failure tolerance requirements are provided in NPR 8705.2, "Human-Rating Requirements for Space Systems." Applicable failure

tolerance requirements in this section of the SAR pertain to all other systems

6.7.4 Failure tolerance requirements for man-rated systems *shall* apply regardless of the results of reliability analysis.

6.7.5 Any program failure tolerance requirements *shall* apply regardless of the results from reliability analysis.

6.7.6 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).

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

6.7.8 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.

6.7.9 Common cause failures *shall* not defeat the redundant design.

Note: The two failure tolerance requirements only apply to nonhuman space systems. Failure tolerance requirements are provided in NPR 8705.2, "Human-Rating Requirements for Space Systems." Applicable failure tolerance requirements in this section of the SAR pertain to all other systems.

6.8 Variances from Two-Failure Tolerance Requirement

When requesting a variance from the two-failure tolerance requirement, the program/project *shall* provide evidence and rationale that:

- a. Two-failure tolerance is not feasible for technical reasons, and
- b. The system or subsystem is designed and certified in accordance with approved consensus standards.

6.9 Probabilistic Risk Assessment (PRA)

6.9.1 General Requirements

6.9.1.1 This section is intended to flow down tailored requirements from NPR 8705.5 for PRA applicable to projects managed by GRC.

6.9.1.2 The program/project systems engineering *shall* work with S&MA to develop the plan for a PRA. A decision to perform a streamlined PRA or no PRA will be documented in the S&MA plan with the program/project rationale.

6.9.2 Criteria for PRA Decision

6.9.2.1 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.

6.9.2.2 A "limited-scope" PRA applies to 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 and Space Science Missions. Predefined system end states may necessitate a top-down fault tree approach rather than event sequence diagrams. This flexibility in analysis approach is available to programs/projects.

6.9.2.3 A “simplified PRA” contains one or more than one undesired top-level events for a system fault tree analysis. A simplified PRA may be performed on Earth Science Missions, Space Science Missions, and technology demonstrations.

6.9.3 PRA Objectives and Ground Rules

6.9.3.1 The maximum allowable probability of occurrence for undesirable consequences *shall* be set by the program or project.

6.9.3.2 The program/project systems engineering and components engineering groups will provide a functional description of system components and a functional flow chart showing the sequence of operation (inputs and outputs).

6.9.3.3 Ground rules for both scope and detail should be developed and reviewed by the PM and PM’s designated representatives and the cognizant S&MA organization.

6.9.4 Application of PRA

6.9.4.1 Weaknesses and vulnerabilities identified by the PRA that can adversely impact safety and mission success *shall* be addressed by the program/project.

6.9.4.2 The program/project engineers *shall* recommend controls (preventive and mitigating features and compensatory measures) needed to reduce the probability of system failures impacting mission success and safety.

6.9.4.3 Information on design that is required to update PRA models and analyses *shall* be provided by design and systems engineering.

6.9.5 Requirement for an Integrated Process

A project’s PRA Integrated Process *shall*:

- a. Assure review by System Safety and Reliability Engineering.
- b. Assure S&MA disciplines will provide information and data to PRA practitioners.

6.9.6 PRA Management

6.9.6.1 Each program/project that is required to perform a PRA *shall* track the progress of the PRA activity against major milestones.

6.9.6.2 At major milestone reviews, progress toward not exceeding the maximum allowable probability of occurrence for loss of crew, loss of mission, or system failure *shall* be assessed.

Chapter 7. Quality Assurance (QA) Requirements

7.1 General Requirements

7.1.1 The program/project *shall* maintain an effective QA program, which assures that quality requirements are met through control of design, operations, processes, procedures, testing, and inspection, and that provides mission success assurance for the defined crew safety, technical, programmatic, regulatory, and other stakeholders' objectives (e.g., do-no-harm) and that is commensurate with the program's or project's risk posture. See Chapter 9 for software product requirements.

7.1.2-Project Managers *shall* develop the QA program that addresses the requirements within NPR 8735.2C and herein as a minimum.

7.1.3 Program/project work *shall* be performed in accordance with the quality system requirements of SAE AS9100, "Quality Management Systems- Requirements for Aviation, Space and Defense Organizations."

7.1.4 Every program/project *shall* develop a QA plan. The QA plan is designed to be a 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 SMAP.

7.1.5 The Project Manager *shall* include requirements in the Project QA program for development and delivery of QA implementation plans by the suppliers that address the requirements of NPR 8735.2C, section 4.1.7 Quality Implementation Plans.

7.1.6 Programs/projects *shall* address the requirements of NPR 8735.2C, Section 6.4 Quality Assurance Program Stability.

7.2 Quality Assurance Organization

7.2.1 Program and/or project managers are responsible for the quality of their assigned products and services, including planning and budgeting for implementation of Government contract quality assurance functions, and provision of personnel resources.

7.2.2 The program/project *shall* designate an individual who is responsible for directing and managing the QA program.

7.2.3 The program/project *shall* make functional assignments to implement each element of the quality program.

7.2.4 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.

7.2.5 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 not be reduced by other considerations, such as the influence of engineering changes, rework, or rescheduling.

7.3 Configuration Management (CM) and Verification

7.3.1 All documents, drawings, and revisions which define and verify the system *shall* be kept under configuration control. See section 10.4 of this document for software configuration control.

7.3.2 The program/project's CM system *shall* be capable of documenting that as-built hardware conforms to the design documentation.

7.3.3 A CM plan *shall* be developed, which will specify responsibilities, and as a minimum, address the following:

- a. Identification of configuration items, which *shall* be baselined and controlled, including specifications and procedures.
- b. Formation of a Configuration Control Board to review baselined items, and to review changes to controlled items, which *shall*:
 - (1) Include the duties of the board, along with responsibilities, and be based on the complexity of the design and be specified in the CM plan.
 - (2) Include the required membership of the board, including Safety & Mission Assurance (S&MA), and be based on the complexity of the design, and be specified in the CM plan.
 - (3) Require the completion of an as-built list that documents the final versions of the components contained in the flight system, along with verification that all testing and changes have been properly completed in both documentation and the system.
 - (4) Include records of all changes made to the system once the configuration items have been baselined.
 - (5) If redline changes are allowed, include requirements to define and control their use and be included in the CM Plan.

7.3.4 The system configuration items *shall* be placed under configuration control and baselined at the earliest possible time, but no later than the time hardware is considered to be in a flight-like configuration and/or by CDR

7.3.5 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.

7.3.6 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.

7.3.7 Inspection records *shall* indicate the revision level with which the item has been fabricated, inspected, and/or tested.

7.3.8 Evidence *shall* be provided specifying compliance with the as-built documentation as a basis for acceptance.

7.4 Identification and Traceability

7.4.1 The program/project *shall* establish a procedure that identifies and tracks each part by a unique part or type number, consistent with the CM system, and:

- a. Be capable of retrieving the identification and serialization record beginning at the subassembly level.
- b. 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.
- c. For identification and serialization data lower than that for subassemblies, maintain in the manufacturing and processing records part number, original manufacturer, serial number, and lot date code information.
- d. Allow identification and traceability controls be able to be cross-referenced to objective evidence of conformance (i.e., hardware quality records) including certificates of quality conformance, production history, qualification and verification results, and usage history.

7.5 Procurement and Contract Quality Assurance Requirements

7.5.1 All procurements *shall* include the appropriate QA requirements for the task, in accordance with NPR 8735.2, with emphasis on section 5.2 Minimum Quality Management System (QMS) Requirements for External Suppliers

7.5.2 The procurement system *shall* address requirements flow down in accordance with NPR 8735.2, section 5.1 Requirements Flow Down.

7.5.3 In accordance with NPR 8735.2, Section 4.3.5 Supplier Risk Assessment and Selection, the following requirements *shall* be included in the QA program:

- a. In addition to the requirements in NPR 8735.1, the NASA Supply Chain Insight Central (SCIC), https://meta.gsfc.nasa.gov/IntelexLogin/Intelex/Application/SCIC/Home/Forms/SCIC_Home/View/35c4daf4-038a-4b82-a674-c5434fe80b34 is used for supplier prescreening. Additional supply chain risk management processes may also be used such as certified or qualified supplier lists and risk assessments based on previous or current Government Contract Quality Assurance (GCQA) activities. This requirement cannot be flowed down to non-NASA project offices.
- b. A pre-award supplier audit, assessment, survey, or equivalent, is used to evaluate supplier risk where no prior record can be referenced in SCIC or in a Government or NASA Center supplier qualification or certification system, or where the prior audit, assessment, survey or GCQA records are older than three years. This requirement cannot be flowed down to non-NASA project offices.

7.5.4 Program/project offices and Government QA organizations *shall* perform Government contract QA for acquisitions in accordance with FAR Part 46, NFS Part 1846, SAE AS9100 Section 7.4.3, and NPR 8735.2, with emphasis on section 7.2 Performing Contract Administration Quality Functions. Standard second-party QA surveillance functions that *shall* be performed are listed in NPR 8735.2,

Section 4.5.1 k.

7.5.5 Government Mandatory Inspection Points (GMIPs) *shall* be determined and assigned in accordance with the requirements of NPR 8735.2, Section 5.7, and GLP-QEA-8735.2, Requirements for Establishing GMIPs.

7.5.6 Quality System Evaluations of contractors *shall* be performed in accordance with the requirements specified in NPR 8735.2C, section 5.5 Supplier Audits and Assessments.

7.5.7 The results of audits *shall* be documented in a report to project management, where the official report becomes a project record. The SMA will work with project management to assure corrective actions are taken to correct deficiencies, prevent recurrence and are verified by NASA where appropriate.

7.5.8 If inspections, tests, or processes need to be verified at the manufacturer/supplier's plant, the procurement document *shall* so indicate.

Note: For such second-party QA surveillance activities, use of a sampling plan versus inspecting 100 percent of the subject population, will be based on an assessment of the likelihood of nonconformance and impact to personnel, including crew, operations personnel, production personnel, and to mission success. Examples of when such inspections, tests, or verifications may be considered include:

- a. 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. (i.e., a complex item per 48 CFR § 46.203)*
- b. When the manufacturer/ supplier has the environment or test equipment needed to perform verifications and it is not technically and economically feasible for the buyer to perform the tests verifications.*
- c. When the history of the manufacturer/supplier shows risk.*
- d. When qualification testing is to be performed by the manufacturer/ supplier.*

7.5.9 The following *shall* be met either through inclusion of the requirement in the procurement or through evaluation by the project engineer and S&MA team in order to manage risk associated with suppliers' design and process changes:

- a. The procurement will require suppliers report design and process changes to NASA.
- b. Suppliers will requalify changed processes unless otherwise agreed to by NASA.
- c. For changed designs and processes, loss of product traceability to requirements will be evaluated by project engineering and S&MA.

7.5.10 Federal Acquisition Regulations (FAR) References for Government Acceptance of Product

Government acquisitions *shall* address the requirements of NPR 8735.2C, 5.8 Federal Acquisition Regulations (FAR) References for Government Acceptance of Product.

7.5.11 Government Rights to Inspect

When appropriate, purchase orders *shall* include a statement, such as FAR clause 52.246-3(c), which assures that the Government has the right to inspect and test any or all of the work included in the purchase order, at all places and times, including the period of manufacture, and in any event before acceptance.

7.5.12 Receiving Inspection

7.5.12.1 The program/project *shall* develop and implement a receiving inspection process, which ensures that purchased products comply with procurement documents.

7.5.12.2 This process *shall* ensure that purchased products are not accepted into inventory until after it has been verified that they conform to the specified purchase requirements.

7.5.12.3 The receiving inspection system may include physical inspections, tests, nondestructive evaluation, and data analysis, and *shall* assure that:

- a. Documentation is reviewed to verify that purchased products comply with purchase requirements.
- b. Inspections and/or tests are performed in accordance with written procedures for selected components to verify performance.
- c. Identification of acceptance, or nonconformance status, of purchased products is documented. All nonconforming items *shall* be segregated for disposition.
- d. Receiving inspection and test records are maintained.
- e. Protective measures for cleanliness, electrostatic discharge, handling, packaging, and shipping are implemented.

7.5.13 Contractor Surveillance (see Section 2.7, Contractor Surveillance)

7.5.13.1 The QA Surveillance Plan(s) (QASP) *shall* be used to document how acquirers (e.g., Government project offices, prime contractors) will conduct second-party, in-process QA surveillance, both for activities that do and do not require mandatory approval (i.e., Mandatory Inspection Point (MIP)) to proceed to the next production step. Suppliers' QASPs may be stand-alone documents or contained in the quality implementation plan or in QMS documentation. For Government project offices preparing QASPs, see <https://sma.nasa.gov/sma-disciplines/qualityfor QASP work aids>.

7.5.13.2 Selection of parallel QA surveillance techniques versus mandatory inspection points, and the types of surveillance techniques, *shall* be selected based on the criticality of the product or process attribute.

7.5.14 Delegation of Government Contract Quality Assurance (GCQA) Functions to Non-NASA Federal Agencies

Non-NASA Federal agencies may be delegated authority to perform GCQA functions on a reimbursable, in-kind, or non-reimbursable basis as formally agreed to in an agency-to-agency memorandum of understanding (MOU). See NPR 8735.2, Chapter 8, for uses of Statements of Work (SOW) (i.e., LODs) to communicate the nature of the delegated work and the minimum information

required by NPR 8735.2, section 7.2.6.

Note 1: The DCMA is an example of an agency that performs delegated GCQA functions on NASA's behalf. See NPR 8735.2, Chapter 8, for requirements specific to delegations to the DCMA.

Note 2: Final product acceptance, denoted by signature approval, is defined as an inherently governmental function and may only be performed by Federal Government employees.

7.6 Control of Fabrication Activities

A fabrication and assembly flow process *shall* be developed and implemented that covers operations from start of fabrication to end item completion and includes:

- a. Inspection and test points and all special processes to be used.
- b. Controls that only conforming components are released and used during fabrication.
 - (1) Verifications and tests defined in the engineering documentation will be used to confirm that the materials and parts considered to be critical items conform with their relevant specifications and requirements prior to their installation into the next higher level of assembly.
 - (2) Verifications and tests defined in the engineering documentation will be used to confirm that consumed materials, used when manufacturing or processing critical items, conform with their relevant specifications and requirements prior to use (e.g., gasses, flux, solvents, inks, ESD protective containers).

7.6.1 Fabrication and Inspection Requirements

Suitable fabrication and inspection requirements *shall*:

- a. Be used based on the complexity and expected environment of the program/project.
- b. Ensure all drawings meet the requirements of American Society of Mechanical Engineers (ASME) y14.5
- c. Ensure only released prints, approved in accordance with the configuration control plan, are used for the manufacture of the qualification and flight hardware.

7.6.2 Control of Assembly, Inspection, and Test Activities

7.6.2.1 The program/project *shall* plan and conduct an assembly, inspection, and test program which controls fabrication, assembly, and testing of flight systems, and demonstrates that drawing and specification requirements are met.

7.6.2.2 The assembly, inspection, and test plans *shall* be approved prior to work being performed on flight articles.

7.6.2.3 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.

7.6.2.4 Each inspection and test *shall* be traceable to the person performing the task and the date.

7.6.2.5 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.

7.6.3 Assembly, Inspection, and Test (AIT) Procedures

7.6.3.1 All work and inspections performed on flight hardware, PLDs, and software *shall* be conducted with approved procedures per the CM plan.

7.6.3.2 Proper planning *shall* be done to ensure orderly and timely inspections are performed at all levels of assembly and tests.

7.6.3.3 The AIT procedures *shall*:

- a. Be written for all flight system operations
- b. Contain the degree of detail in the procedures commensurate with the complexity of the operation. Drawings may stand alone as assembly procedures as appropriate.
- c. Include written confirmation that procedures were followed
- d. Assure any deviations from the procedures is properly approved and recorded per the CM plan.
- e. Indicate for each system operation the individual responsible for its accomplishment. The individual's name and date the operation was performed will be recorded.

7.6.3.4 Procedures *shall* include, as applicable:

- a. The revision level of the document
- b. The nomenclature of the article
- c. Instructions for qualified personnel to perform the work
- d. Characteristics to be inspected or tested
- e. Accept/reject criteria
- f. Special considerations regarding handling, measuring, testing, equipment, standards, safety, and environment.

7.6.3.5 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.

7.6.3.6 Procedures *shall* be traceable to product and process technical specifications (i.e., attributes of the design, of process controls, of the verifications and tests, and of pass/fail criteria not otherwise specified in the design specifications).

7.6.3.7 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.

7.6.3.8 Procedures *shall* require the recording of equipment identification and calibration due dates

for all calibrated instruments used.

7.6.3.9 During testing, QA assures that testing/ inspection is performed with the approved procedures. After testing/ inspection, QA assures that the results and data are complete and traceable to the appropriate test article. The records of this activity *shall* be kept in sufficient detail to verify and evaluate the status of all articles and materials tested/inspected.

7.6.3.10 Test and inspection results *shall* be fully traceable to the item configuration specifications, the verification requirements, the item identifications (e.g., lot number, serial number), and the details that are unique to the production flow (e.g., date, operator, production line).

7.6.3.11 For integration activities, the requirements of NPR 8735.2C, section 4.6 Integration and Test (I&T) *shall* be complied with to assure quality controls are used and quality conformance is sustained during integration and test (I&T) processes.

7.6.3.12 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 the 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 plan *shall* be created (may be part of SMAP) based on project criticality, and include activities to maintain fastener traceability, perform fastener testing (typically to verify chemical composition and strength), and provide controlled fastener storage.
- b. In addition to the requirements that all flight fasteners undergo lot testing to verify chemical composition, heat treat, strength, and lot variability, fracture critical fasteners *shall*:
 - i. Require NDE or proof testing of each fastener
 - ii. Require separate storage from the other fasteners.
- c. The requirements for fastener integrity are levied through NASA-STD-8739.14, or through NASA-STD-5020 which has NASA-STD-8739.14 as a child requirement. S&MA has the Technical Authority for NSAS-STD-8739.14. Any tailoring of the standards by the Fastener Integrity Plan requires S&MA Technical Authority approval.

7.6.4 Training for Personnel

7.6.4.1 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. This includes specialized training and procedures for inspectors when the verification method is nonstandard and/or depends on unique methods for product handling, using inspection equipment, or discerning defects (e.g., microstructural analyses of coupons or samples, evaluating optical coatings, nondestructive evaluation (NDE), pre-cap inspection of hybrid microcircuits).

7.6.4.2 Personnel performing specific assigned tasks *shall* be qualified on the basis of appropriate education, training and/or experience, as required.

7.6.4.3 The PM *shall* specify in the program/project plan the training needs for the program/project.

7.6.4.4 Appropriate records of training *shall* be maintained (see Section 7.17.)

7.6.5 Evaluation and Control of Process Specifications and Procedures

7.6.5.1 All specifications and procedures for processes *shall* be evaluated to ensure compliance to program/project requirements.

7.6.5.2 Special processes, with which the quality cannot be ensured by inspection alone, *shall* be given special attention, including process qualification, as to the controls and methods of verifying the adequacy of the process.

7.6.5.3 Manufacturability risks for non-standard, unqualified, and low-maturity designs and manufacturing methods where technical specifications of form, fit, function, process control, or verification techniques are not established, *shall* be identified and managed.

7.6.5.4 The developer's QA organization *shall* assure all processes are adequate for the stated purpose.

7.6.5.5 The following list of special process and inspection documents are requirements for all NASA GRC flight hardware:

Table 7.1 NASA Adopted Technical Standards for Quality Engineering and Quality Assurance

Document Number	Title
NASA-STD-5009	Nondestructive Evaluation Requirements for Fracture Critical Metallic Components
NASA-STD-6016	Standard Materials and Processes for Spacecraft
NASA-STD-8739.1	Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
NASA-STD-8739.4	Crimping, Interconnecting Cables, Harnesses, and Wiring or IPC IPC/WHMA-A-620B-S, Space Applications Electronic Hardware Addendum to IPC/WHMA-A-620B
NASA-STD-8739.5	Fiber Optics Terminations, Cable Assemblies, and Installation
NASA-STD-8739.6	Implementation Requirements for NASA Workmanship Standards
NASA-STD-8739.10	Electrical, Electronic, and Electromechanical (EEE) Parts Assurance Standard
NASA-STD-8739.12	Metrology and Calibration
NASA-STD-8739.14	NASA Fastener Procurement, Receiving Inspection, and Storage Practices for NASA Mission Hardware
ANSI/ESD S20.20-2014	ESD Association Standard for the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices)
IPC J-STD-001GS	Joint Industry Standard, Space Applications Electronic Hardware Addendum to IPC J-STD-001G Requirements for Soldered Electrical and Electronic Assemblies (Chapter 10 of IPC J-STD-001GS does not apply)
IPC/WHMA-A-620C-S	Space Applications Electronic Hardware Addendum to IPC/WHMA-A-620C
NAS 412 Revision 1	Foreign Object Damage/Foreign Object Debris (FOD) Prevention

SAE GEIA-STD-0005-1A	Performance Standard for Aerospace and High-Performance Electronic Systems Containing Lead-free Solder
SAE GEIA-STD-0005-2A	Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High-Performance Electronic Systems
SAE AS5553C	Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition.
SAE AS6174A	Counterfeit Materiel, Assuring Acquisition of Authentic and Conforming Materiel

7.6.5.6 The projects control of processes *shall* include:

a. Compliance with the following for control of Pb-free materials (reference section 5.9):

- (1) Conformance by suppliers with the criteria of SAE-GEIA-STD-0005-1A and SAE-GEIA-STD-0005-2A using control level “2C.”
- (2) Extension of Pb-free controls to non-critical items when necessary to mitigate the risk of metal whisker growth on, and liberation from, a non-critical item affecting critical item performance during a mission.

b. Fasteners and fastener supplier selection comply with NASA-STD-8739.14. See NASA-STD-8739.14 for further explanation of hardware applicability (reference section 7.6.3.12).

c. Other requirements imposed by the program/project as deemed necessary.

7.6.6 Bonded Storage

7.6.6.1 The program/project *shall*:

- a. Maintain a controlled bonded storage area, which is capable of storing flight material, parts, and assemblies.
- b. Define the level and type of environmental control based on the specifics of the flight material, parts, and assemblies being stored.
- c. Ensure that environmental control minimally protect the flight items from excessive temperatures and humidity, and from contamination.
- d. Implement electrostatic discharge (ESD) controls for ESD sensitive parts as defined in Section 7.8.

7.6.6.2 The bonded storage area *shall*:

- a. Have controlled access applicable to the type of system being stored
- b. Include a documentation system adequate to identify and track the flow of parts in and out of bonded storage.
- c. Have the ability to segregate materials, assemblies, qualified components, accepted systems, limited-life items, and nonconforming components.
- d. Include traceability by part number, original manufacturer, serial numbers, and lot date code for parts and components in controlled storage.

7.6.7 Records of Inspections and Tests

Records *shall*:

- a. 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.
- b. Be kept for each component, subassembly, and assembly, based on their complexity.
- c. Assure as the product is integrated, the next higher-level assembly documentation references all integrated subassemblies or subsystems by positive configuration identification.
- d. Document all actions taken on the component
- e. Provide for easily accessible total operating time of the component under control.
- f. Be traceable to:
 - (1) The personnel who performed the function.
 - (2) The date the assurance work was performed.

7.7 Contamination Control

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

7.7.1 Contamination Control Plan (CCP)

7.7.1.1 The program/project *shall* prepare and implement a CCP:

- a. That describes methods for controlling contaminants and verifying that they have been prevented or abated such that the hardware will meet performance requirements.
- b. Will be submitted for approval by the GRC project management and the GRC program/project assurance manager prior to work being performed on flight hardware.

7.7.1.2 Analyses, procedures, standards, processes, and specifications referenced in the CCP *shall* be available for review at the developer's facility.

7.7.1.3 The CCP *shall*:

- a. Be generated in accordance with the guidelines of ASTM E1548 (2009), Standard Practice for Preparation of Aerospace Contamination Control Plans.
- b. Define contamination allowances for performance degradation of contamination-sensitive systems, and rationale for allowable levels, such that, even in the degraded state, the system will meet its mission objectives.
 - (1) 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.
 - (2) Allowable levels serve as a basis for the measurements to be taken to control contamination.

- (3) The contamination allowable will 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. Describe methods for controlling contamination and for ensuring that the contamination allowance is not exceeded.
- d. 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.
- e. Identify controls to be exercised in preparing test facilities, such as the thermal-vacuum chamber and fixtures, and include:
 - (1) 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.
 - (2) Appropriate pretest measurements, monitoring methods to be used during the tests, and post-test measurement.
- f. Require bake-outs of hardware be based on the materials evaluation and use environment. When required, the parameters of bake-outs (e.g., temperature, duration, pressure) will be individualized depending on the materials used, the fabrication environment, and contamination allowance.
- g. Address the contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, and bagging (e.g., antistatic film materials).
- h. Include clean room standards and personnel training.

7.8 Electrostatic Discharge (ESD) Prevention

7.8.1 The developer *shall* plan, implement, and maintain an ESD control process that meets or exceeds the ESD Association ANSI/ESD S20.20 requirements and NASA-STD-8739.6, Section 7. The NASA GRC is structured such that ESD requirements are the responsibility of individual projects to implement and assure. As such, it is the responsibility of each project to define and implement ESD controls, through individual project ESD control plans.

7.8.2 The GRC procedure GLP-QE-8739.2, ESD Control Plan, applies to all GRC organizations and personnel (civil servants, onsite contractors, or visitors) who are involved in the design, purchase, handling, storage, shipping/receiving, inspection, repair, fabrication or operation of flight and flight associated hardware, or mission critical and elements thereof containing ESD sensitive items.

7.9 Nonconformance and Problem Reporting and Control

7.9.1 The program/project's Nonconformance and Problem Reporting and Control system *shall*:

- a. Report nonconformances and failures through a documented problem reporting and corrective action (PRACA) system.
 - (1) In-house programs/projects will handle PRACA through the GRC CAPA System (GLP-Q-1280.2, Corrective and Preventive Action), or a comparable system approved by S&MA.
 - (2) An outside contractor may maintain its own PRACA system with approval of the PM and CSO.

- b. Implement the PRACA system during the development phase within the program/project team, or as otherwise specified in the SMAP.
- c. Initiate the PRACA review process and review board at the same time as the implementation of the PRACA system.
- d. Include documentation of problem, segregation of nonconforming material, traceability of material or part, disposition of problem, root cause corrective action, verification of corrective action, and trending to help prevent similar nonconformances.
- e. Describe the problem review process including the use of review boards and the problem report tracking and distribution process in the project SMAP.
- f. For contracted projects, require the contractor to review/notify NASA project management within 48 hours of occurrence of 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).

7.9.2 Problem reports *shall* include as a minimum:

- a. Description of problem.
- b. Traceability of nonconforming item.
- c. Analysis of root cause of problem.
- d. The disposition of the problem, and supporting rationale.
- e. Description of corrective action, and
- f. Corrective action follow-up.

7.9.3 Review Boards

A review board (i.e., Material Review Board (MRB) or Failure Review Board) *shall*:

- a. Be operated with the responsibility of reviewing all problem reports.
- b. Include the following:
 - (1) Quality or reliability representative (chairman for MRBs).
 - (2) Engineering representative.
 - (3) PM or his/her representative (necessary for failure board only).
 - (4) Government representative, if other members are contractor personnel.
 - (5) Other participants as appropriate, such as consideration of representatives for manufacturing process controls, engineering and system design, reliability, and programmatic risk.

Note: This requirement does not prescribe the number or types of consultants engaged by the review board but instead is intended to convey that technical and programmatic considerations must be addressed by the review board to achieve a risk-balanced disposition.

- c. Have the responsibility for:
 - (1) Investigation/analysis of the cause(s) for the nonconformance.
 - (2) Determining the disposition of the submitted problem.

- (3) The following are dispositions which may be assigned for nonconforming items:
 - (a) Rework - action taken on a nonconforming product so that it will fulfill the specified requirements.
 - (b) Repair - action taken on a nonconforming product so that it will fulfill the intended usage requirements, although it does not conform to the originally specified requirements. Customer concessions and communications is required to be documented.
 - (3) Regrade - action taken to revise the classification of a nonconforming product to use on a less stringent application.
 - (4) Return to vendor - action taken to return nonconforming product to the vendor in accordance with contract provisions.
 - (5) Use as is - approving the use of a nonconforming product without resorting to rework or repair, following the waiver process, or after documenting customer concessions and communications.
 - (6) Scrap - action taken on nonconforming product to make it unusable and to remove it from unintended use.
- (4) Approving all standard repair procedures.
- (5) Specifying the engineering and quality controls to be used, including process qualification if applicable, when using board-recommended rework or repair processes that are non-standard and when the consequences of process failure would have a negative impact to safety or programmatic success.
- (6) Assuring that both the standard and non-standard processes and procedures used for rework and repair are documented and controlled. Training may be required to ensure successful implementation of rework or repair processes.
- (7) Investigating and addressing nonconformance scope of impact including those that cut across multiple systems.
- (8) Ensuring that remedial and preventative actions are properly addressed.
- (9) Ensuring that excessive repairs do not compromise the component's reliability and quality.

7.9.3.4 The board *shall* maintain review board records that track and record the progress of the investigation and disposition until closure. Records associated with nonconformance review board activities are an element of acceptance data packages and provide the program/project the ability to research and evaluate mission risks, product and material traceability, and final hardware configuration.

7.9.3.5 The board *shall* assure that the requirements of NPR 8735.2C, section 6.3.2, are complied with for nonconformances associated with products or processes from external suppliers that are associated with high levels of risk to mission success objectives (e.g., crew safety, technical, programmatic, regulatory) and that require supplier-led root cause and corrective action (RCCA) processes to resolve the nonconformance and to prevent its reoccurrence.

7.9.4 Waivers and Deviations

7.9.4.1 The acceptance of any nonconformance affecting flight acceptance, safety, or mission success *shall* require an approved waiver or deviation.

7.9.4.2 The process defined in GLPR 7120.5.20, GRC Project Deviation/Waiver Process, *shall* be used to document and approve any deviations or waivers.

7.9.4.3 For contracted projects, the contractor's SMAP *shall* describe the process for submission, review, and disposition of a request for waiver or deviation.

7.9.4.5 Program, project, and operations/institutional managers collectively *shall* provide official program/project waiver, deviation, or exception documentation with rationale and justification and a risk mitigation plan for relief of NPR 8735.1 to the Chief, Safety and Mission Assurance, Center Director, and the Center GIDEP/NANADARTS Coordinator for concurrence.

7.9.5 Control of Nonconforming Product

7.9.5.1 Methods *shall* be established and implemented for identifying and segregating any nonconforming item to the extent possible.

7.9.5.2 The nonconformance and any immediate action(s) taken *shall* be documented, and the nonconformance dispositioned, per the requirements of 7.9.1.

7.9.5.3 For project work performed on-site at GRC, that require formal control of nonconforming items, and that is supported by Code QEA Quality Assurance, GLWI-QEA-8730.25 will be used.

7.10 Alert Information

7.10.1 The NANADARTS system includes GIDEP ALERTs, SAFE-ALERTs, Problem Advisories, and Agency Action Notices.

7.10.2 The program/project *shall*:

- a. Review NASA Parts Advisories and 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 FMEA and CIL and disposition for design reviews.
- b. Assure that the status of closed loop activity (resulting from NANADARTS database searches and applicable NANADARTS reports) is reported at milestone reviews.
- c. Report discrepant parts, suspect counterfeit parts, and/or components that are within the scope of NANADARTS to the GRC GIDEP/NANADARTS coordinator (Program and Project Assurance Division), who will prepare and submit the Failure Experience report to NANADARTS or issue the NASA Parts Advisory per NPR 8735.1.

7.10.3 A contractor may use its own GIDEP representative to prepare and submit the GIDEP Failure Experience report, but *shall* inform the GRC PM, CSO, and GRC GIDEP/NANADARTS Coordinator of the problem and provide them with an advance copy of the report.

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

- a. GIDEP home page - <https://www.gidep.org/>

b. NANADARTS home page - <https://nanadarts.nasa.gov/>

7.10.5 Refer to GLWI-QEA-8735.1 for further information on how NPR 8735.1 is implemented at GRC.

7.11 Inspection and Test of Stored Limited-Life Hardware

7.11.1 A test plan *shall*:

- a. Be developed, which assures that limited-life items stored or stocked have not been degraded or damaged during storage.
- b. Address proper handling, including environmental conditions, to mitigate damage or prolong life, and testing to assure the stored items meet required specifications.

7.11.3 Limited-life items shall:

- a. Be considered nonconforming, and handled in accordance with section 7.9, when not meeting the requirements set forth in the plan.
- b. Be identified on a list and a log of their remaining of their remaining life, with the list and log being actively maintained.

7.12 Metrology

7.12.1 Only properly calibrated instruments and tools in accordance with NASA-STD-8739.12 (and for GRC, also GLPR 8730.6) *shall* be used to assemble, test, inspect, and verify flight hardware.

7.12.2 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.

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

7.13.1 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 turnover at integration.

7.13.2 For preservation of product, hardware item quality and accumulated quality pedigree *shall* be preserved during production, operations, handling, storage, and shipping by process controls that prevent:

- a. Inadvertent damage due to unapproved operations or failure to follow procedures.
- b. Chemical and particulate contamination.
- c. Incursion of Foreign Objects Debris (FOD). The requirements of NASA-STD-6016 require suppliers to develop a FOD control plan that is consistent with the guidance found in NAS 412 Revision 1.
- d. Poor tool, fixture, and equipment controls.
- e. Nonconforming environmental controls, both of ambient and test environments.

- f. Nonconforming item handling, packaging, storage, and shipping materials and processes.
- g. Damage due to uncontrolled ESD. The technical standards in Table 4.1 define the minimum ESD sensitivity level for which a control program is required.

7.13.3 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.

7.13.4 Also all accompanying documents *shall* have been properly identified as to inspection status with the appropriate inspection stamps.

7.14 Control of Government Property by Contractors

7.14.1 When supplied in accordance with the provisions of the contract, government property *shall* be controlled and accounted for by the contractor.

7.14.2 The contractor *shall* be responsible for, at minimum:

- a. Upon receipt, examine components to detect damage that may have occurred in transit.
- b. Inspect for quantity, completeness of shipment, and proper shipping documents.
- c. Provisions for protection, maintenance, calibration, periodic inspection, and controls necessary to prevent damage or deterioration during handling, storage, installation, or shipment.

7.14.3 Any property that is found damaged, malfunctioning, or otherwise unsuitable for use *shall* be processed in accordance with government procedures and Section 7.9.

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

7.15 System Acceptance Review

7.15.1 Prior to GRC-developed hardware being shipped from GRC, or prior to the hardware turnover to the project integrator or customer, a System Acceptance Review *shall* be held.

7.15.2 Upon successful completion of the System Acceptance Review, including completion of all open work assigned as a result of the System Acceptance Review, the PM *shall* initiate the GRC Certificate of Flight Readiness (CoFR) signature cycle.

7.15.3 The GRC CoFR signature page and GRC CoFR formats are found in Appendix D. Copies of the signed form should be kept in permanent program/project records according to the program/project's records management system.

7.15.4 The GRC has traditionally held a Pre-Ship Review (PSR) for shuttle missions. Following is a description of the PSR process which may be helpful when tailoring a project's SAR process:

- a. Pre-Ship Review (PSR): The Pre-ship Review is a comprehensive review of end item quality, verifies the

completeness of the specific end products in relation to their expected maturity level, and assesses compliance to stakeholder expectations. The PSR examines the system, its end products and documentation, and test data and analyses that support verification. It also ensures that the system has sufficient technical maturity to authorize its shipment to the designated operational facility or launch site.

- b. The PSR is a two-part review: the Engineering PSR (PSR-1) and the Executive PSR (PSR-2).
 - (1) PSR-1: Ensure project compliance with applicable GRC and project level requirements for successful implementation and control of all development, test, V&V, and documentation activities prior to shipment of GRC space flight hardware. Chaired by CE/Technical Lead Engineer, or another individual as designated by the PM, with board consisting of Code L, Q, and M (K for Aero projects) Division/Line Management representatives. Goal: Approval to proceed
 - (a) End Product Audit: Quality Assurance inspection of the project documentation (e.g., V&V documentation, Test reports, etc.) Goal: QA Report
 - (b) Bench Review: Quality Assurance physical inspection of the hardware and shipping documentation. Goal: QA Signing DD-250 (Outside Contractor Build) OR QA Signing DD1149 (GRC In-House Build)
 - (2) Executive PSR-2: Final review of the project readiness and results in a decision by Center Management to ship. This responsibility is delegated to the PSR-2 Board, and the review is chaired by a representative from code M (K for Aero projects), with Board members from the Code L and Q. Goal: Final Approval to Ship

7.16 Product Acceptance / Acceptance Data Package (ADP)

7.16.1 All spaceflight projects managed by GRC *shall* have an ADP prepared for end-item deliverables.

7.16.2 Flight and qualification units *shall* meet the Acceptance/ADP requirements. Each project *shall* define the applicability of acceptance/ADP requirements for developmental units.

7.16.3 The ADP *shall* include the following, as a minimum:

- a. As-built configuration list in accordance with Section 7.3.
- b. Statement of as-built configuration's traceability to requirements.
- c. List of as-built parts used in accordance with Chapter 5.
- d. List of materials and processes used in accordance with Chapter 3.4.7.
- e. Log books, including total operating and repair times, and cycle records.
- f. Status of all verification items with a list of open items and rationale for the items being open.
- g. Records of successful completion of all required inspections and tests, including incoming inspections, GMIPs, and acceptance tests.
- h. Listing, status, and remaining life of limited-life items.
- i. Results of Flight Acceptance Tests.

- j. Listing and status of all nonconformance, failure, or problem reports, and their associated dispositions (i.e. rework, repair, use-as-is).
- k. Record of non-conformance dispositions of use-as-is and any residual configuration or qualification traceability gaps.
- l. Record of agreement between the Government and the prime contractor for acceptance of nonconforming items (for additional information, see Nonconforming supplies or services, 48 CFR § 46.407.(b).(2)). This requirement applies for production at all levels of the supply chain.
- m. Listing of waivers and deviations affecting flight acceptance, safety, and mission success.
- n. Cleanliness certification.
- o. Certification of flight software acceptance in accordance with Chapter 10.
- p. Parts and materials conformance certifications.
- q. Photographs for subassemblies and components prior to permanent seal of their enclosure or installation into the next higher level of assembly when they can no longer be inspected.
- r. Shipping and handling instructions.
- s. Terms and conditions for exercising applicable warranties (for additional information, see NFS1846.7, Warrantees).

7.16.2 Product certification and Government acceptance requirements *shall* be flowed down to external suppliers for use with their sub tier suppliers (for additional information, see Subcontracts, 48 CFR § 46.405).

7.16.3 Processes *shall* be established for collecting, delivering, and retaining objective evidence of item or process conformance by the project and by the supplier (e.g., end item data package, Acceptance Data Package (ADP)). For additional information, see Contract administration office responsibilities and Contractor responsibilities, 48 CFR §§ 46.104(c), 105(4).

7.16.4 Product Acceptance Data Package Review

The ADP reviews *shall* be used to ensure that the documentation contains records of, or traceability to, objective evidence of product conformance, risks that have not been fully mitigated, and accepted nonconformances and requirement waivers. The ADP reviews are conducted with a level of rigor that is commensurate with the item's complexity, criticality, and known risks and issues associated with nonconformances and waivers. Highly integrated systems may require formal project-level, multidisciplinary reviews in order to certify or accept the hardware. A QA review of quality documentation and records may be sufficient for less complex items.

7.17 Control of Quality Records

7.17.1 The program/project *shall* establish and maintain documented procedures for identification, collection, indexing, access, filing, storage, maintenance, and disposition of quality records.

7.17.2 The quality records *shall* be maintained to demonstrate conformance to specified requirements and

the effective operation of the quality system.

7.17.3 Pertinent quality records from the subcontractor *shall* be an element of these data.

7.17.4 Record-keeping methods provide the research expediency needed to minimize programmatic impacts from known and emerging quality problems (e.g., GIDEP alerts, counterfeit items, fraudulent material certifications, faulty designs, and qualification failures).

7.18 Launch and Mission Initiation Operations

When programs/projects include launch and mission initiation operations, the launch and mission initiation operations *shall* comply with the requirements of NPR 8735.2, 4.7 Launch and Mission Initiation Operations.

Chapter 8. Continuous Risk Management (RM)

Note: The NPR 8000.4 provides the requirements for risk management for the Agency, its institutions, programs and projects. 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.

8.1 Introduction

8.1.1 The 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.

8.1.2 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.

8.2 Risk Informed Decision Making (RIDM)

8.2.1 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.

8.2.2 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.

8.3 Continuous Risk Management (CRM)

8.3.1 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:

- a. Assess continually what could go wrong (risks).
- b. Determine which risks are important to deal with.
- c. Implement strategies to deal with those risks.
- d. Assure and measure the effectiveness of the implemented strategies (or mitigations).

8.3.2 The RIDM and CRM

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.

8.3.3 Institutional Risks

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.

8.4 General Requirements

8.4.1 The NASA directive NPR 7120.5, NASA Space Flight Program and Project Management Processes and Requirements, provides the basic RM requirements that are applicable to all programs and projects. The Center's GLPR 8000.4 implements the RM provisions of the NPR 7120.5. Both documents require that each NASA program and project *shall* 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.

8.4.2 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 projects.).

8.4.3 The program/project *shall* develop a RM plan in accordance with the provisions of NPR 7120.5 and NPR 8000.4, and:

- a. Be developed during the formulation phase and executed/ maintained throughout the life cycle of the program/project.
- b. Can be a standalone document or as part of the program/project plan

- c. Document how risks will be managed: the processes, activities, responsibilities, milestones and resources associated with RM.

8.4.4 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.

8.5 Initial Risk Management Training

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.

8.6 Implementation

8.6.1 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.

8.6.2 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.

8.6.3 Identifying Risks

8.6.3.1 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.

8.6.3.2 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.*

8.6.3.3 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.

8.6.4 Analyzing Risks

8.6.4.1 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.

8.6.4.2 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.

8.6.5 Planning

8.6.5.1 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 implementing 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:

- a. Is it my risk or responsibility?
- b. What approach can I take with this risk?
- c. How much and what should I do with this risk?

8.6.5.2 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.

8.6.5.3 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.

8.6.5.4 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.

8.6.5.5 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.

8.6.6 Risk Tracking

8.6.6.1 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. Risks *shall* be:

- a. Tracked and reevaluated periodically. (The actual time 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.)
- b. Tracked and monitored to verify the mitigation is reducing the risks as planned.
- c. Be actively communicated to the appropriate level (as defined in program/project documentation) in a timely manner.
- d. 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 for any recommendation from higher level reviews.

8.6.6.2 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.

8.6.7 Risk Control

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.

8.6.8 Communication and Documentation

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. 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.

8.6.8.1 Risk Database

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).

- a. 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.
- b. 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.

8.6.8.2 Risk Reporting

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 9: Flight Software Assurance and Software Safety (SASS)

9.0 Flight Software Assurance and Software Safety (SASS)

9.1 SASS Procurement Planning

For GRC procurement activities, as part of SMA’s early involvement in requirements development, software assurance should be an integral part of procurement discussions as applicable. If SMA or Software Assurance is not involved during procurement formulation or not invited to pre-award activities, or if activities have commenced, Software Assurance or SMA notifies the project of which requirements need to be addressed or are at risk of being deficient.

9.2 Responsibilities

9.2.1 GRC Software Assurance Engineer

The GRC Software Assurance Engineer *shall*:

- a. Develop and formally document a tailoring matrix of NASA-STD-8739.8 SASS requirements to capture planning, implementation intent, identify deliverables, activities, and tasks that will inform contract requirements, agreements, memorandums, or grants pre-award.
- b. Assure the GRC CSO/Project SMA Lead and GRC SA Technical Authority review the tailoring before informing contract requirements and deliverables pre-award. Tailoring of NASA-STD-8739.8 is performed in accordance with NPR 8715.3, General Safety Program Requirements and NASA-STD-8709.20, Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements.
- c. Define which tasks, activities, and contract deliverables from the NASA-STD-8739.8 compliance matrix are necessary for the flight software project pre-award are to be completed by the contractor and what monitoring activities will be completed by the Government pre-award.
- d. Assure the following Government insight contract deliverables are specified in the contract requirements and contract deliverable list for all flight software projects unless tailored by the program or project as applicable in the NASA-STD-8739.8 compliance matrix and agreed with by the Software Assurance Technical Authority (Table 9-1):

Table 9-1. Required Software Assurance and Software Safety Quality and Defect Data

SASS Deliverable	Delivery Schedule	Responsible Party	Dependencies
Software Quality and Defect List	Each major milestone until software release	Supplier	Modifiable Source Code Access Access to the number of software

			nonconformances at each severity level for each software configuration item
Static Code Analysis Result(s) by severity	Design Review through each milestone until release	Supplier	Modifiable Source Code Access or access to SCA results and configuration
High Severity Software Non-conformance Root Cause Analysis	As identified and defined by the project. As necessary.	Supplier	Access to the number of software nonconformances at each severity level for each software configuration item

- e. Assure the Government has access to modifiable supplier source code, training, and tools to analyze or assess the source code if these are not listed as deliverables.
- f. Assure high severity problem reports or non-conformances related to software are documented and addressed.
- g. Where needed, assure Static Code Analysis Results includes cybersecurity vulnerabilities and weaknesses.
- h. Include all software safety requirements in NASA-STD-8739.8, as the basis for contracts, memoranda of understanding, and other documents related to software in accordance with NPR 8715.3, General Safety Program Requirements.
- i. Assure Government insight and approval activities are defined in the SAP or SMAP.
- j. Plan intent to complete SASS artifacts for all flight software projects as applicable in the program or project NASA-STD-8739.8 compliance matrix if not specified as a data deliverable.
- k. Include the following data deliverables in the procurement pre-award activity for approval (Table 9-2):

Table 9-2. Required Software Assurance and Software Safety Data Deliverables

SASS Deliverable	Delivered and evaluated with proposal	Delivered for government approval at contract start	Required	Milestone Schedule
Software Assurance and Software Safety Plan	Yes	Yes	Yes. May also be incorporated into the Safety and Mission Assurance Plan (SMAP)	Final at PDR or equivalent

Software Safety Analysis	Yes, if a hazard analysis or hazard report(s) are available	Yes, if a hazard analysis or hazard report(s) are available	Yes and updated at each major program or project milestone until test readiness review or equivalent.	Each milestone until test readiness review or equivalent
Software Assurance Requirement Analysis	No	No	See the programs or projects NASA-STD-8739.8 requirements mapping matrix.	Software Requirements Review, SRR, and PDR
Software Assurance Design Analysis	No	No	See the programs or projects NASA-STD-8739.8 requirements mapping matrix.	Every milestone until CDR
Audit Reports	No	No	See the programs or projects NASA-STD-8739.8 requirements mapping matrix.	See Project Software Assurance Plan
Cyclomatic Complexity metrics	No	No	Yes	Updated at every milestone

- l. Address and notify the project manager of any program or project NASA-STD-8739.8 or NPR 7150.2 requirement or deliverable gaps or deficiencies during pre-award.
- m. Use the software safety requirements in NASA-STD-8739.8 as a basis for requirements, contracts, memoranda of understanding, documents, and deliverables.

9.2.2 GRC Project Manager

The GRC Project Manager *shall*:

- a. Plan Software Assurance and Software Safety per NASA-STD-8739.8 in accordance with NPR 8715.3, General Safety Program Requirements.
- b. Use the software safety requirements in NASA-STD-8739.8, as the basis for contracts, memoranda of understanding, and other documents related to software in accordance with NPR 8715.3, General Safety Program Requirements.
- c. Address Independent Verification and Validation (IV&V) in accordance with GLPR 8739.1 Chapter 2 or NASA-STD-8739.8 and determine if IV&V requirements contained in NASA-STD-8739.8 are applicable using NPR 8705.5, Risk Classification for NASA Payloads.

9.3 Flight SASS Planning and Implementation

9.3.1 GRC Project Manager

The GRC Project Manager *shall*:

- a. Execute responsibilities in accordance with GLPR 8739.1, Chapter 1.
- b. Plan and address Software Independent Verification and Validation per NASA-STD-8739.8 in accordance with NPR 8715.3.
- c. Plan and address IV&V requirements contained in NASA-STD-8739.8 or GLPR 8739.1 Chapter 2 if applicable.

9.3.2 GRC Software Assurance Engineer

The GRC Software Assurance Engineer *shall*:

- a. Plan and implement Software Assurance and Software Safety per GLPR 8739.1, or as defined in the contract, agreement or grant.
- b. Develop and maintain a Software Assurance Plan (SAP) per NASA-HDBK-2203, including software safety.
- c. Tailor requirements in accordance with NASA-STD-8739.8, NPR 8715.3, General Safety Program Requirements and NASA-STD-8709.20, Management of Safety and Mission Assurance Technical Authority (SMA TA) Requirements.
- d. Define which requirements in the NASA-STD-8739.8 requirements matrix will be completed by the Government and which will be completed by the contractor or supplier.

Note: The outputs and responsible person may be different, Government insight and acceptance activities and tasks are defined in the Software Assurance Plan for contractor/supplier vs Government expectations. Surveillance and monitoring will be consistent with SMA insight and assurance plans.

e. Reference GLWI-QEA-8750.8, GLWI-QEA-8750.1, and GLWI-QEA-8750.7 in order to assist with planning and implementing Government Software Assurance and Software Safety activities and requirements.

f. Plan SASS audits in the P/P/F project Software Assurance Plan.

(1) A configuration management audit is recommended before each software baseline or software release. At a minimum software configuration audit(s) are required to be performed before a ground test, flight test, or software verification.

(2) Perform audits on software development processes and practices at least once every two years.

(3) Plan applicable audits as defined in the projects NASA-STD-8739.8 requirements matrix.

- g. Plan software safety test witnessing activities including travel and cost information to supplier sites if applicable.
- h. Request training and tools required for Static Code Analysis to the P/P/F as applicable.
- i. Communicate and work with the Safety and Mission Assurance Project Lead for the P/P/F to update the Safety and Mission Assurance Plan or Software Assurance Plan to fulfill the applicable requirements per the Requirements Mapping Matrix and any agreed upon changes as applicable.

Note: The contracting officer or contracting officer representative can be contacted on any potential adjustments or modifications that may be needed to applicable contracts to meet the modified requirements if a system or subsystem development evolves to meet a higher or lower software classification as defined in NPR 7150.2.

- j. Provide project or program software quality and defect metrics or data to grc-swa@mail.nasa.gov as applicable.

Note: For example: Coding rule violations, software defect metrics, and code quality.

- k. Document which processes, standards, or requirements are being followed if the program or project elects to not use NASA-STD-8739.8 or GLPD 8739.1.

- l. Plan and implement to either produce or accept delivery of the following SASS artifacts throughout the program and project lifecycle:

Note: The preparer of the following artifacts may use recommended content defined in the NASA Software Engineering and Assurance Handbook NASA-HDBK-2203 (www.swehb.nasa.gov) and NASA-STD-8739.8 if not otherwise defined in contract deliverables, statements of work, or agreements.

Table 9.1 - Recommended SASS Artifacts and lifecycle milestones

SASS Artifact(s)	Pre-award/ Pre-agreement	System Requirements Review	Preliminary Design Review	Critical Design Review	Test Readiness Review	Flight Readiness Review
SASS SOW, PWS, MOA, MOU requirements	Initial	Update	Update	Update		
Software Assurance Requirements Analysis			Baseline	Update	Update	Update
SASS Requirements Tailoring Matrix	Preliminary	Initial	Baseline	Update	Update	Update
Software Assurance Plan	Preliminary	Initial	Baseline	Update	Update	Update
Software Safety Analysis	Preliminary	Initial	Baseline	Update	Update	Update

Software Assurance Design Analysis			Preliminary	Baseline	Update	Update
Static Code Analysis Result(s)			Initial	Update	Update	Update
SASS Audit Reports		As defined in the Project's SAP or SMAP	As defined in the Project's SAP or SMAP	As defined in the Project's SAP or SMAP	As defined in the Project's SAP or SMAP	As defined in the Project's SAP or SMAP
SASS Issue/Defect/Concern/Risk/Non-conformance List		Initial	Update	Update	Update	Update
Cyclomatic Complexity Metrics		Initial	Update	Update	Update	Update

- m. Report high severity software non-conformance in accordance with GLP-Q-1280.2 or identify an equivalent reporting process for suppliers or contractors to use to the extent specified or referenced in their contracts, grants, or agreements
- n. Determine if Software IV&V requirements contained in NASA-STD-8739.8 are applicable using NPR 8705.4 Risk Classification for NASA Payloads, and will tailor as needed and in accordance with 10.2.2.a.3 of this document.

CHAPTER 10. Flight Programmable Logic Assurance

Note: If the project includes software as defined in NPR 7150.2 in any part of the programmable logic device development process, then Chapter 10, Software Assurance and Software Safety shall be followed for any use of software.

10.1 Flight Programmable Logic Assurance Procurement Planning

For GRC procurement activities, as part of SMA's early involvement in requirements development, software assurance should be an integral part of procurement discussions as applicable. If SMA or Software Assurance is not involved during procurement formulation or not invited to pre-award activities, or if activities have commenced, Software Assurance or SMA notifies the project of which requirements need to be addressed or are at risk of being deficient.

10.2 Responsibilities

10.2.1 GRC Project Manager

The responsible GRC Project Manager will plan and address Programmable Logic and Programmable Logic Device requirements and deliverables for pre-award activities.

10.2.2 GRC Project Quality Engineer

The GRC Project Quality Engineer *shall*:

- a. Include the following questions as part of the project planning, contract initiation, Request For Information (RFI) or equivalent:
 - (1) Does the program or project plan on using programmable logic devices?
 - (2) Does the project plan to have programmable logic device(s) that include or contain software as defined in NPR 7150.2?
 - (3) Does the program or project plan on developing a programming file contained in non-volatile memory or volatile memory that is stored on a Field Programmable Gate Array (FPGA) or used with an FPGA?
 - (4) Does the program or project plan on using, previously used, or is currently using High-level Synthesis (HLS)?
 - (5) Does the program or project plan on using, previously used, or is currently using a programming language, software toolchain, or tool (C, C++, SystemC, MATLAB, VHDL Coder, etc.) to generate VHDL, Verilog, RTL, or instruction set architecture?
- b. Work with Software Assurance Engineering, determine if the project needs to follow NPR 7150.2 and NASA-STD-8739.8 based on the RFI responses or equivalent information.
- c. Recommend that the project or supplier includes requirements for activities and deliverables to show compliance with a programmable logic device standard or process.

- (1) For example, NASA-HDBK-4008 and NASA-HDBK-8739.8
 - (2) The PLD's do not include software and a hardware description language is not autogenerated from a software programming language.
- d. Perform a safety assessment in accordance with NASA-HDBK-8739.23 chapter 6.3 if NASA-HDBK-4008 is used as a guide for pre-award activities. The PLD safety assessment on the device(s) is updated at each major milestone of development until the release version of the PLD is placed onto the flight circuit board.
- e. Use the PLD Assessment Form found in Appendix E of NASA-HDBK-8739.23 to document the PLD assessment score, assurance effort, safety criticality, and mission criticality values and placed into the projects official records if NASA-HDBK-4008 is used as a guide for pre-award activities.
- f. Define which programmable logic assurance tasks, activities, and contract deliverables are necessary for the flight programmable logic project pre-award are to be completed by the contractor and what monitoring activities will be completed by the Government pre-award.
- (1) Refer to NASA-HDBK-4008 and NASA-HDBK-8739.8.
 - (2) The following data deliverables are examples of project requirements and deliverable data requirements pre-award for all flight programmable logic projects:

Table 10.1 - Recommended Deliverables for Projects using NASA-HDBK-4008

PLD Deliverable	Milestone Schedule	Responsible	Dependencies
PLD Configuration Management Plan	As defined by the project	Supplier	NASA-HDBK-4008
PLD Verification Plan	As defined by the project	Supplier	NASA-HDBK-4008
Safety Assessment	As defined by the project	Supplier	NASA-HDBK-8739.23 chapter 6.3
PLD Assurance Plan	As defined by the project	Quality Engineer	NASA-HDBK-8739.23
PLD Classification	As defined by the project	Supplier	NASA-HDBK-4008
PLD Assurance Classification	As defined by the project	Quality Engineer	NASA-HDBK-4008

10.3 Flight Programmable Logic Assurance Planning and Implementation

This section is only applicable if a program or project utilizes NASA-HDBK-4008, Programmable Logic Devices (PLD) Handbook, as a guide and to the extent specified or referenced in their contracts, grants, or agreements.

10.3.1 GRC Project Manager

10.3.1.1 The GRC Project Manager will consider following the requirements if the flight program or project is following NASA-HDBK-4008 guidance:

- a. Plan, implement, and maintain a PLD development program in accordance with the NASA-HDBK-4008.
- b. Request a Quality Engineer (QE) to be assigned to the project for programmable logic assurance.
- c. Classify the PLD(s) per Appendix C in NASA-HDBK-4008.

10.3.1.2 The GRC Project Manager will plan and implement a Programmable Logic Device Configuration Management Plan.

- a. Developed by the project/ program or included in the project management to describe items to be configuration managed and the configuration management process for these items.
- b. The following items should be configuration managed: plans and procedures, requirements documents, schematics, Hardware Description Language (HDL) code, test benches and other test code, simulation code and scripts, COTS IP modules, test inputs (scripts, files, etc.), test outputs (data files), and development tools.

10.3.1.3 The GRC Project Manager will:

- a. Define Verification and validation (V&V) processes, plans, and implementation to demonstrate that the developed PLD meets system and subsystem requirements while correctly providing the necessary functionality.
 - (1) Detailed Verification Planning is contained in the NASA-HDBK-4008 Chapter 9.
 - (2) Other verification activities that occur during other development phases based on PLD classification will include, but are not limited to, HDL (Hardware Description Language) reviews, walkthroughs or inspections, unit testing, audits of the HDL development processes/ products, final HDL acceptance, and system testing.
- b. Perform a safety assessment in accordance with NASA-HDBK-8739.23 chapter 6.3. The PLD safety assessment on the device(s) is updated at each major milestone of development until the release version of the PLD is placed onto the flight circuit board.
- c. Use the PLD Assessment Form found in Appendix E of NASA-HDBK-8739.23 to document the PLD assessment score, assurance effort, safety criticality, and mission criticality values and placed into the project's official records.
- d. Identify reliability methods and activities that are customized in accordance with the results of the PLD assessment using NASA-HDBK-4008 Appendix C by the project, the Design Lead Engineer, and Quality Engineer.
- e. Identify fault tolerance requirements through the use of failure modes and effects analysis, fault tree analysis, errors trending, or other proven reliability analysis and tools.
- f. Assure that the reliability activities for the developed PLD(s) does not contribute to a total system failure as a result of external errors, or other input conditions.

10.3.2 Quality Engineer

A GRC Project Quality Engineer will:

- a. Plan and implement programmable logic assurance using NASA-HDBK-8739.23, “NASA Complex Electronics Handbook for Assurance Professionals,” as a guide if NASA-HDBK-4008 is used by the program or project.

- b. Concur with the PLD classification(s).

- c. Concur on the PLD safety assessment in accordance with NASA-HDBK-8739.23 Chapter 6.3.

- d. Perform a PLD assurance classification to classify each PLD device into Hi/ Moderate/ Low Assurance Level or effort using the score generated using Table 5 in Appendix C of NASA-HDBK-4008.

- e. Develop a PLD Assurance Plan defining the assurance activities appropriate to its assurance classification level.

Appendix A. Definitions

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).

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.

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

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.

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.

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

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.

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.

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.

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.

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

Continuous Risk Management (CRM). 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.

Credible Failure Mode. A failure mode that is possible.

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.

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

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.

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.

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

Discrepancy. See Nonconformance.

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

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

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

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

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.

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.)

Experiment. See Payload.

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

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.

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.

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

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.

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

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.)

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

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.

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.

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.

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

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.

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

Inspection. The process of comparing an article with requirements.

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

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).

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.

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

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).

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.

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.

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

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

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

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

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.

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.

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

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.

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

Primary Structure. That part of a flight vehicle or element that sustains the significant applied loads and provides main load paths for distributing reactions to applied loads. Also, the main structure that is required to sustain the significant applied loads, including pressure and thermal loads, and that, if it fails, creates a catastrophic hazard. If a component is small enough, and in an environment where no serious threat is imposed if it breaks, then it is not primary structure.

Prototype Hardware. See Hardware.

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.

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.

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

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

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

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

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.

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.

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

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.

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.

Structural. Pertaining to structure.

Structure. All components and assemblies designed to sustain loads or pressures, provide stiffness and stability, or provide support or containment.

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

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

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.

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.

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.

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.

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.

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.

Verification. See Performance Verification.

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.

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

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

ABPL	As-Built Parts List
ADP	Acceptance Data Package
ADPL	As-Designed Parts List
AIAA	American Institute of Aeronautics and Astronautics
AIT	Assembly, Inspection and Test
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ATD	Advanced Technology Development
BMS	Business Management System
CCP	Contamination Control Plan
CDR	Critical Design Review
CE	Complex Electronics
CIL	Critical Items List
CM	Configuration Management
CoFR	Certificate of Flight Readiness
COPV	Composite Overwrapped Pressure Vessels
CORR	Corrosion Resistance
COTS	Commercial Off-the-Shelf
CPARS	Corrective and Preventive Action Reporting System
CRM	Continuous Risk Management
CSCI	Computer Software Configuration Item
CSO	Chief Safety and Mission Assurance Officer
CVCM	Collected Volatile Condensable Material
DFMR	Design for Minimum Risk
EDMS	Electronic Document Management System
EEE	Electrical, Electronic and Electromechanical
ELV	Expendable Launch Vehicle
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ERB	Engineering Review Board ESD. Electrostatic Discharge
EXPRESS	EXpedite the PRocess of Experiments to Space Station

FAR	Federal Acquisition Regulation
FCA	Functional Configuration Audit
FEM	Finite Element Model
FLAM	Flammability
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FS	Factor of Safety
FS&GS	Flight Systems and Ground Support
FTA	Fault Tree Analysis
GCQA	Government Contract Quality Assurance
GFE	Government Furnished Equipment
GIDEP	Government-Industry Data Exchange Program
GLM	Glenn Manual
GLPD	Glenn Policy Directive
GLPR	Glenn Procedural Requirements
GMIP	Government Mandatory Inspection Points
GRC	Glenn Research Center
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
HDL	Hardware Description Language
HTV	H-II Transfer Vehicle
HW	Hardware
IPC	Institute for Interconnecting and Packaging Electronic Circuits
ISS	International Space Station
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KSC	Kennedy Space Center
LOD	Letters of Delegation
LSE	Lead Systems Engineer
M&P	Materials and Processes
MEFL	Maximum Expected Flight Level
MIL-STD	Military Standard
MS	Margin of Safety
MSFC	Marshall Space Flight Center

MTTR	Mean Time to Repair, Restore or Replace
NASA	National Aeronautics and Space Administration
NDE	Nondestructive Evaluation
NFS	NASA Federal Acquisition Regulation Supplement
NHLBB	Non-Hazardous Leak Before Burst
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NPSL	NASA Parts Selection List
NSTS	National Space Transportation System (Shuttle)
PCA	Physical Configuration Audit
PCE	Project Chief Engineer
PDR	Preliminary Design Review
PIL	Parts Identification List
PLD	Programmable Logic Device PM. Project Manager
PPAD	Program and Project Assurance Division
PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action
QA	Quality Assurance
QAAR	Quality Audit, Assessment and Review
QASP	QA Surveillance Plan
R&M	Reliability and Maintainability
RAM	Reliability, Availability and Maintainability
REDAA	Requirements Evaluation and Documentation Assessment and Analysis
RFCB	Responsible Fracture Control Board
RIDM	Risk Informed Decision Making
RM	Risk Management
RMIT	Risk Management Implementation Tool
RSS	Root-Sum-Square SA. Software Assurance
SAR	Space Assurance Requirements
SCS	Safety-Critical Structures
SCIC	Supply Chain Insight Central
SEE	Single Event Effects
SE&I	Systems Engineering and Integration

SEMP	Systems Engineering Management Plan
SERB	Safety and Mission Assurance Engineering Review Board (ref: GLWI-Q-8700.3, Safety and Mission Assurance Engineering Review Board (SERB))
S&MA	Safety and Mission Assurance
SMAD	Safety and Mission Assurance Directorate
SMAP	Safety and Mission Assurance Plan
SMARTS	Safety and Mission Assurance Requirements Tracking System
SR&QA	Safety, Reliability and Quality Assurance
SSTP	System Safety Technical Plan
STS	Space Transportation System (Shuttle)
SW	Software
TML	Total Mass Loss
TRL	Technology Readiness Level
V&V	Verification and Validation
WFF	Wallops Flight Facility
WPTR	Worst-case Predicted Temperature Range

Appendix C. Verification Matrix

This Verification Matrix to the Space Assurance Requirements (SAR) can be used to satisfy successful completion of the program and project reviews, verifications 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

GLPR Section	Requirement Statement	Project Implementation Intent Existing Project Doc/Section	Compliance			Justification
			Full	Partial	None	
2.1.1	S&MA lead/CSO <i>shall</i> assist PM in accomplishing assurance requirements and has direct access.					
2.1.2	S&MA program <i>shall</i> operate concurrently with all other elements					
2.1.3	S&MA program <i>shall</i> be in place throughout the life cycle of the program or project					
2.1.4	S&MA program <i>shall</i> apply to all work					
2.1.5	Project Safety and Mission Assurance Plan (SMAP) <i>shall</i> go through a Safety and Mission Assurance Engineering Review Board (SERB)					
2.2	Safety and Mission Assurance Plan (SMAP)					
2.3	Use of Deviations					
2.4	Use of Previously Designed, Fabricated, or Flown Systems					
2.5	Storage Requirements for Suspended Projects					
2.6	Assurance Status Reports					
2.7	Contractor Surveillance					
2.8	GRC Assurance Review Requirements					
2.9	Mishap Reporting and Investigation					
2.10	Safety, Health, and Environment					
3.1	Design and Verification - General Requirements					
3.2	Overall Verification Program					
3.3	Electrical Requirements and Verification					
3.4	Structural and Mechanical Requirements					

3.4.1	General Requirements					
3.4.2	Safety-Critical and Fracture-Critical Structures					
3.4.3	Structural Loads					
3.4.4	Factors of Safety					
3.4.5	Margins of Safety					
3.4.6	Fracture Control					
3.4.7	Materials and Processes Selection, Implementation and Control Requirements					
3.4.8	Pressurized Systems					
3.4.9	Strength Testing					
3.4.10	Vibroacoustics					
3.4.10.1	General requirements					
3.4.10.2	Component Random Vibration Testing					
3.4.10.3	Workmanship					
3.4.10.4	Stowed Components					
3.4.10.5	Retesting of Reflight Hardware					
3.4.10.6	Additional Vibroacoustic Testing					
3.4.11.1	Shock (Mechanical and Pyro) General					
3.4.11.2	Shock Flight Acceptance					
3.4.12	Mechanical Functions					
3.4.12.1	Qualification Testing					
3.4.12.2	Flight Acceptance Testing					
3.4.13	Pressure Profile					
3.4.14	Mass Properties					
3.5	Electromagnetic Compatibility (EMC) Requirements					
3.6	Radiation Requirements					
3.7	Vacuum, Thermal and Humidity Requirements					
3.7.1	Worst-Case Predicted Temperature Range					
3.7.2	Validation of Thermal Properties					
3.7.3	Compliance with Requirements					
3.7.4	Testing Levels					
3.7.5	Applicable Testing					
3.7.5.1	Thermal Cycling					

3.7.5.2	Thermal Balance Testing					
3.7.5.3	Humidity					
3.7.6	Applicable Analysis					
3.8	Flight System Performance Acceptance Test Requirements					
3.8.1	Burn-In Tests					
3.8.2	Mission Simulation Test					
3.8.3	End-to-End Compatibility Test					
3.9	Ground Support Equipment (GSE)					
4	System Safety					
4.1	Introduction					
4.2	System Safety Planning					
4.3	Hazards Analysis					
4.4	Failure Tolerance					
4.5	Design for Minimum Risk and Similar Approaches					
4.6	Internal GRC Review of Safety Products					
4.7	Requirements Applicability					
5	EEE and Mechanical Parts Control					
5.1	General Requirements					
5.2	EEE Parts Selection and Screening					
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	Derating					
5.2.6	Radiation Hardness					
5.2.7	Corona and Arcing					
5.2.8	Inspection Prior to Assembly					
5.3	Mechanical Parts Selection and Screening					
5.3.3	Mechanical Parts Control Plan					
5.3.4	Inspection Prior to Assembly					
5.4	Procurement of Parts					
5.5	Parts Storage					
5.6	Storage Life Screening					

5.7	Parts Identification List					
5.8	Parts Risk Evaluation					
5.9	Parts Subject to Metal Whisker Growth					
5.10	Salvaged Parts					
6	Reliability, Availability and Maintainability					
6.1	General Requirements					
6.2	RAM Requirement for an Integrated Process					
6.3	RAM Management					
6.4	RAM Plan					
6.5	RAM Data					
6.6	RAM Report Archives					
6.7	Reliability and Failure Tolerance					
6.8	Variances from Two-Failure Tolerance Requirement					
6.9	Probabilistic Risk Assessment (PRA)					
7	Quality Assurance Requirements					
7.1	General Requirements					
7.2	Quality Assurance Organization					
7.3	Configuration Management and Verification					
7.4	Identification and Traceability					
7.5	Procurement and Contract Quality Assurance Requirements					
7.6	Control of Fabrication Activities					
7.7	Contamination Control					
7.8	Electrostatic Discharge (ESD) Control					
7.9	Nonconformance and Problem Reporting and Control					
7.10	Alert Information					
7.11	Inspection and Test of Stored Limited-life Hardware					
7.12	Metrology					
7.13	Handling, Preservation, Marking, Packaging, Packing and Transportation					
7.14	Control of Government Property by Contractors					
7.15	System Acceptance Review					
7.16	Product Acceptance/Acceptance Data Package (ADP)					
7.17	Control of Quality Records					

7.18	Launch and Mission Initiation Operations					
8	Continuous Risk Management					
8.4	General Requirements					
8.6	Implementation					
9	Flight Software Assurance and Software Safety (SASS)					
9.1	SASS Procurement Planning					
9.2	Responsibilities					
9.3	Flight SASS Planning and Implementation					
10	Flight Programmable Logic Assurance					

10.1	Flight Programmable Logic Assurance Procurement Planning					
10.2	Responsibilities					
10.3	Flight Programmable Logic Assurance Planning and Implementation					

Appendix D. Templates and Forms

D.1 Project Safety and Mission Assurance Plan (SMAP)

The Program and Project Assurance Division, Code QE, of GRC has a template to assist with creating individual project SMAPs. Contact the project Chief SMA Officer or project SMA lead for assistance.

D.2 Certificate of Flight Readiness

 National Aeronautics and Space Administration			
Project Certificate of Flight Readiness (CoFR) Endorsement Signature Sheet			
TITLE	NAME	SIGNATURE <i>N/A - Signature on certificate.</i>	DATE
Director, NASA Glenn Research Center			
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 2061 08/14 (1.0)

*Also sign certificate.

PREVIOUS EDITIONS ARE OBSOLETE.

GLPR 7120.5.30 Appendix D.2

Page 1 of 1

D.3 Certificate of Flight Readiness (con't)

	National Aeronautics and Space Administration	GRC Certificate of Flight Readiness	
<p>At the [redacted] Review, the GRC Management Team has certified that the deliverable hardware requirements related to the GRC area of responsibility have been satisfactorily completed. As of this preship review, there are no constraints related tot 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.</p>			
<p>The GRC Management Team has certified:</p>			
<ul style="list-style-type: none">(1) As-build 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			
[redacted]	[redacted]		
Director, NASA Glenn Research Center	Date		
[redacted]	[redacted]		
Director, Space Flight Systems Directorate	Date		
[redacted]	[redacted]		
GRC Project Manager	Date		

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:

<https://oa.jsc.nasa.gov/OE/SRP/Lists/SRP%20Documents%20%20Requirements/AllItems.aspx>

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): <https://iss-www.jsc.nasa.gov/nwo/apps/edms/web/>

Web sites with ELV User Guides:

Delta II:

<http://www.ulalaunch.com/uploads/docs/DeltaIIPayloadPlannersGuide2007.pdf>

Sea Launch:

<http://www.sea-launch.com/launch/11137>

Atlas V:

<http://www.ulalaunch.com/uploads/docs/AtlasVUsersGuide2010.pdf>

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

Appendix F. References

- a. ANSI/AIAA G-020-1992, “Guide for Estimating and Budgeting Weight and Power Contingencies for Spacecraft Systems”
- b. GLM-QS-1700.1, “NASA Glenn Safety Manual”
- c. GLM-QS-1800.1, “Occupational Health Programs Manual”
- d. GLM-FE-8500.1, “Environmental Programs Manual”
- e. GLWI-QER-8730.6, “Design for Ionizing Radiation”
- f. JSC 23642, “JSC Fastener Integrity Testing Program”
- g. MIL-HDBK-1811, “Mass Properties Control for Space Vehicles”
- h. MSFC-HDBK-670, “General Environmental Test Guideline (GETG) for Protoflight Instruments and Experiments”
- i. MSFC-STD-3012, “Electrical, Electronic, Electromechanical (EEE) Parts Management and Control Requirements for MSFC Space Flight Hardware”
- j. NASA-HDBK-4007, “Spacecraft High-Voltage Paschen and Corona Design Handbook”
- k. NASA-HDBK-5010, “Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware”
- l. NASA-HDBK-7004-C, “Force Limited Vibration Testing” NASA-HDBK-8739.23, “NASA Complex Electronics Handbook for Assurance Professionals”
- m. NASA-STD-5020, “Requirements for Threaded Fastening Systems in Spaceflight Hardware”
- n. NASA-TM-106943, “Preloaded Joint Analysis Methodology for Space Flight Systems”
- o. NASA-TM-86538, “Design and Verification Guidelines for Vibroacoustic and Transient Environments”
- p. NASA TM X-73305, “Astronautic Structures Manual Volume I”
- q. PD-ED-1201, “EEE Parts: De-Rating”
- r. PD-ED-1202, “High Voltage Power Supply Design and Manufacturing Practices”
- s. RSM-2002, Range Safety Manual for Goddard Space Flight Center (GSFC) Wallops Flight Facility (WFF)
- t. S-313-100, “Goddard Space Flight Center Fastener Integrity Requirements”
- u. SAE AS5553, “Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition”

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.
2	10/30/14	Administrative change – extended expiration date from November 3, 2014 to November 3, 2015 in accordance with GLPR 1410.1.
3	11/02/15	A three-month extension was added to continue with the approval process for Revision A, per GLPR 1410.1, Section 1.5a. (from 11/03/2015 to 02/03/2016).
A	3/4/16	This update includes significant technical changes to incorporate such things as the retirement of the STS (Shuttle Program), requirement changes in the applicable documents, and addition of new requirement standards, NPRs, etc. The GLPR update also incorporates changes to correct gaps/findings identified during the Requirements Evaluation and Documentation Assessment and Analysis (REDAA) and the Quality Audit, Assessment and Review (QAAR). Formatting/content requirements/signature authority has been updated in accordance with NPR 1400.1.
Change 1	8/11/17	Administrative change – corrected document numbers from recent BMS changes. Also incorporated parts of GLPR 5340.1 given future cancellation of the document.
B	12/07/2022	<p>Significant changes to Software Assurance and Quality Assurance sections due to major changes in Agency requirements.</p> <p>Chapter 6 inserted into Section 3.4.7. Moved Materials and Processes from Section 6 to Section 3 as a result of the M&P function moving from SMA to engineering.</p> <p>Updated to meet requirements of GLPR 1410.1, including: editorial changes to correct document revisions and clarity.</p> <p>Changed 7.15 Pre-Ship Review (PSR) to System Acceptance Review</p> <p>Removed reference to GLSBU document in P4 and 2.9.a</p> <p>Removed Appendix F. References</p>