MSFC-HDBK-3701
BASELINE
EFFECTIVE DATE: 07/27/2015

National Aeronautics and
Space Administration

George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama 35812

EE11

MSFC TECHNICAL STANDARD

MSFC INTEGRATED ENGINEERING PRINCIPLES HANDBOOK

Approved for Public Release; Distribution is Unlimited

CHECK THE MASTER LIST—
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

DOCUMENT HISTORY LOG

Status (Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Baseline	-	07/27/2015	Baseline Release was authorized by the MSFC Technical Standards Document Control Board (DCB) through the Multiprogram Document Management System (MPDMS). Administrative update 07/28/2015 to correct the OPR code on the cover page.

FOREWORD

This Handbook, produced by the Marshall Space Flight Center (MSFC) Engineering Directorate, documents a broad range of critical engineering principles needed for communication between stakeholders and the engineering community. The principles and guidance contained in this Handbook help define MSFC design practices that have become a part of our engineering excellence. These principles are required to ensure proper technical integration across the entirety of the engineering disciplines at MSFC and products that can be physically integrated during production.

The Handbook is a product of the combined MSFC engineering discipline community, including the Propulsion Systems Department, the Spacecraft & Vehicle Systems Department, the Space Systems Department, the Test Laboratory, the Mission Operations Laboratory, the Materials & Processes Laboratory, the MSFC Chief Engineer’s Office, and the Safety and Mission Assurance organization.

TABLE OF CONTENTS

PARAGRAPH PAGE

1.0 INTRODUCTION 6
1.1 Scope 6
1.2 Purpose 7
1.3 Document Maintenance 7
1.4 Document Change Authority 7
2.0 APPLICABLE DOCUMENTS 8
2.1 Government Documents 8
2.2 Non-Government Documents 8
3.0 DEFINITIONS 9
4.0 DESIGN MARGINS 10
5.0 INTEGRATED ENGINEERING PRINCIPLES 11
5.1 General Principles 11
5.2 Aero Sciences 22
5.3 Electrical Power 22
5.4 Fault Management 23
5.5 Flight Mechanisms 28
5.6 Guidance, Navigation, and Control 28
5.7 Human Systems Integration 28
5.8 Materials, Processes, and Manufacturing 29
5.9 Mechanical Systems 37
5.10 Natural Environments 37
5.11 Nondestructive Evaluation 41
5.12 Operations 41
5.13 Propulsion Systems 47
5.14 Safety, Reliability, and Maintainability 54
5.15 Software 59
5.16 Structures 62
5.17 Systems Engineering 63

5.18 Test 63

5.19 Thermal 65

5.20 Vehicle Management 67

APPENDIX

APPENDIX A DOCUMENTS COMMONLY USED BY THE MSFC ENGINEERING COMMUNITY OF PRACTICE 70

APPENDIX B ACRONYMS AND ABBREVIATIONS 75

TABLE

TABLE I. DESIGN MARGINS COMPARISON 10

TABLE II. FAILURE ISOLATION PER MISSION PHASE 25

1.0 INTRODUCTION

This document provides discipline-specific details associated with design and operation of space flight systems developed at Marshall Space Flight Center (MSFC).

The contents of this document have been selected based on the following criteria:

a. Incorporation of lessons learned that were key to past successes and where deviations from these practices created significant problems.

b. Documentation of the flight design key principles, considering the applications and environments to which the flight systems are subjected.

c. Identification of key data, analyses, evaluation, characteristics, and other information that one discipline needs to provide to enable the success of one or more other disciplines and on which the system integrity is based.

d. Identification, by reference, of the standards used by the MSFC engineering disciplines in their activities.

e. Inclusion of the integration/integrating principles that result in a coordinated/integrated product.

1.1 Scope

This document applies in the design, verification/validation, manufacture, assembly, test, and operation of launch vehicles, spacecraft, payloads, and instruments. The principles of this document apply in all modes of project implementation for those deliverables for which MSFC is responsible, whether the flight system effort is contracted, is a shared responsibility of MSFC and a partner, or is implemented as an “in-house” project.

The principles of this document do not apply to hardware elements that are provided to MSFC by outside entities or that are produced under the control of other National Aeronautics and Space Administration (NASA) Centers, Government agencies, or other nations.

Principles of this document may not be applicable to the design of ground support equipment (GSE) or special test equipment items, such as test fixtures, fluid systems, and piping that are used for ground testing of flight systems and flight system elements.

1.2 Purpose

The purposes of this document are as follows:

a. To define a set of integrated engineering principles and best practices to assist in executing the requirements found in discipline Marshall Procedural Requirements (MPRs) and the technical standards found in Appendix A.

b. To define a set of engineering principles that communicate the character of MSFC flight designs to the MSFC engineering community of practice.

c. To establish a common standard(s) by which project designs and risks can be assessed.

d. To serve as a starting point for technical risk management both in community engagement and assessment.

1.3 Document Maintenance

As the Office of Primary Responsibility (OPR), the MSFC Systems Engineering Management Office/EE11 is responsible for the development and maintenance of this Handbook. The Handbook is reviewed annually to ensure relevance and adequacy of the Center's integrated engineering principles.

1.4 Document Change Authority

The MSFC Systems Engineering Management Office/EE11 is the OPR for this Handbook. Any proposed changes to this Handbook are submitted as necessary to EE11 for disposition.

2.0 REFERENCE DOCUMENTS

This section lists documents cited by principles presented in this Handbook. They contain provisions or other pertinent requirements that are directly related to and necessary for the performance of the activities addressed by this Handbook.

Documents listed in Appendix A are a compilation of standards, specifications, and industry practices that are used by specific engineering disciplines within the MSFC Engineering Directorate and that serve as a point of reference for technical professionals.

2.1 Government Documents

ER01 Memorandum	MSFC Propulsion Systems Designers' Handbook (MPSDH) NOTE: Copies available from ER/MSFC Propulsion Systems Department
ES22 Memorandum	Transportation and Handling Limit Load Factors NOTE: Copies available from ES/MSFC Thermal & Mechanical Analysis Branch.
MSFC-RQMT-3479	Fracture Control Requirements for Composite and Bonded Vehicle and Payload Structures
MSFC-STD-3620	MSFC Electrical, Electronic, Electromechanical (EEE) Parts Obsolescence Management and Control Requirements
MSFC-STD-3676	Development of Vibroacoustics and Shock Design and Test Criteria
Organizational Issuance QD-R-001	Failure Mode and Effects Analysis and Critical Items List

2.2 Non-Government Documents

2.2.1 Batelle Memorial Institute

MMPDS-08	Metallic Material Properties Development and Standardization (MMPDS)

2.2.2 SAE International

CMH-17	Composite Materials Handbook

3.0 DEFINITIONS

Criticality 1 or 1R - Items whose failure or malfunction could result in loss of vehicle, life, or serious injury. For additional information on criticality definition, see Organizational Issuance QD-R-001, Failure Mode and Effects Analysis and Critical Items List.

Design Margin - A recommended value that is the difference between the maximum possible value and the maximum expected value for a technical resource. Margins typically change as the design matures.

Ground Support Equipment - Mechanical and electrical hardware for handling, servicing, calibrating, and maintaining the launch vehicle and for replacing Line Replaceable Units (LRUs), limited-life items, shipping covers, and Remove Before Flight items.

Heritage - Space hardware and software designed, manufactured, processed, or integrated for one type of architecture or purpose are considered heritage or modified heritage when they are proposed for use in a different architecture or for a different purpose.

Mission Critical - Item or function that must retain its operational capability to assure mission success.

Off-the-Shelf Component - Hardware or software that is pre-built, that is already developed and requires minor interface configuration changes, if any, and that can be used to speed the development of a low-cost solution while minimizing program risk.

Safety Critical - A term describing any condition, event, operation, process, equipment, or system that could cause or lead to severe injury, major damage, or mission failure if performed or built improperly or allowed to remain uncorrected.

Should - The use of the term “should” in this document denotes a good practice and is recommended but not required.

Will - The use of the term “will” in this document denotes expected outcome.

4.0 DESIGN MARGINS

Table I, Design Margins Comparison, presents, as best practice, typical margins for various functions at critical milestones in the program/project lifecycle. The table consolidates data from multiple sources and can be used for ease of reference.

Table I. Design Margins Comparison

Function	SRR	PDR	CDR	System Integration	Launch
Electrical/Electronics					
Timing	25%	20%	15%	10%	Program Specific
Bus Utilization	25%	20%	15%	10%	Program Specific
Fiber Optic Link	4 dB	4 dB	4 dB	4 dB	Program Specific
Spare channels	25%	20%	15%	10%	Program Specific
Mass	25%	20%	15%	10%	Program Specific
Thermal	*	*	*	*	Program Specific
Telemetry and Command Hardware Channels	25%	20%	15%	10%	Program Specific
Connector Pinouts	N/A	30%	10%	10%	5%
RF Link Margin	3 dB	3 dB	3 dB	3 dB	3 dB
Bit Error Rate	1.00E-06	1.00E-06	1.00E-06	1.00E-06	1.00E-06
Dry Mass (5.0)	30%	20%	20%	5% (DCR)	0
System Power/Energy	30%	20%	15%	10% (DCR)	10%
Operating Margins					
RAM	N/A	N/A	50%	40% (TRR)	30% (AR)
EEPROM	N/A	N/A	20%	20% (TRR)	10% (AR)
CPU	N/A	N/A	N/A	35% (TRR)	25% (AR)

AR	Acceptance Review	PDR	Preliminary Design Review
CDR	Critical Design Review	RAM	Random Access Memory
CPU	Central Processing Unit	RF	Radio Frequency
DCR	Design Certification Review	SRR	System Requirements Review
EEPROM	Electrically Erasable Programmable Read Only Memory	TRR	Test Readiness Review
N/A	Not Applicable		

*See section 5.19 for thermal margins.

There are other margins, but these are not tied to milestones and are not included in this table.

5.0 INTEGRATED ENGINEERING PRINCIPLES

These principles apply to launch vehicles, spacecraft, payloads, and instruments.

5.1 General Principles

5.1.1 Similar Components

5.1.1.1 In design trades, similarity may only be used when each of the following criteria is met:

a. Engineering evaluation reveals that design configurations between the item under assessment and the similar item would produce the same results if the qualification activity was performed on the item under assessment.

b. The similar item was designed for and qualified to equal or higher environmental levels, e.g., thermal, stress, than those required for the item under assessment.

c. The item under assessment was built by the same manufacturer using the same material and manufacturing processes and the same quality control procedures as the similar item.

d. Similarity assessment undergoes an independent evaluation by a technically qualified person or group other than the person(s) performing the similarity assessment. Similarity will not be used when either of the following conditions exists:

1. The similar item used in the assessment was itself verified/validated using similarity as the method.
2. Items whose criticality is 1 or 1R.

e. Assessments will be made regarding technical interfaces (hardware and software), performance, and the environments to which the unit has been previously qualified, including electromagnetic compatibility (EMC), radiation, and contamination.

f. The compatibility of the design with parts quality requirements is also to be assessed.

g. All non-compliances will be identified, documented, and addressed either by modification to bring the component into compliance or by formal waivers/deviations for accepted deficiencies.

h. If a qualification-by-similarity approach is agreed upon by the supplier and MSFC, the data used to demonstrate similarity will not exceed one generation, i.e., not extrapolated across multiple programs.

i. The item can be demonstrated to be subject to the same environments, natural and induced (electromagnetic interference (EMI), thermal, pressure, structural, vibrational, human interface, etc.,) in its integrated configuration as those for which it was previously qualified.

5.1.1.2 Similarity may not be applied in the following situations:

a. Qualification by similarity is not acceptable if the current vendor is not the original vendor, i.e., current vendor is the rights owner only.

b. All fluid system components will be qualification tested. Qualification by similarity is not recommended.

Note: Examples of fluid systems include liquid feed systems, gaseous pressurization and purge systems, coolant systems, hydraulic systems, etc.

5.1.2 Trending of system/component performance will be conducted throughout the lifetime of the program.

Note: The trend data collection should begin in the development phase to obtain as much data as soon as possible. The data are valuable for determining dispersions to be applied to component and system models used for vehicle requirements development.

Rationale: Since the population of systems/components is comparatively low, it is important to collect, store, and trend data throughout the lifetime of a program, as this information can be important when design decisions relating to the use of heritage hardware occur.

5.1.3 Design will include producibility analyses that address constraints and capabilities of materials, machining equipment, inspectability, and humans.

5.1.4 System design will consider the uncertainties and variations in system parameters.

Rationale: Subsystems and functional capabilities (structural, aero thermal, etc.) should at least cover for the expected range of possible variations for the mission to be successful. It is never sufficient to use nominal parameters. These uncertainties and variations should be appropriately discriminated as either epistemic (there is a specific value, but the actual value is not known) or aleatory (randomly varies for each launch or component, but the variation is unknown) and accordingly included in the models and analyses.

5.1.5 When practical, space-flight hardware is tested, verifying its performance, as individual components (either by the supplier or by the recipient) for accuracy and function, functionally within the system, and functionally as a system.

Rationale: This tiered testing demonstrates that each component will work as needed before its integration, so that integrated testing will be much quicker and less costly. The functional testing shows the system will work. Testing as a complete system finds issues in the overall integration and system interactions that cannot be found otherwise.

5.1.6 When practical, required redundant circuit paths will use separated connectors and separate cable harnesses for electrical and physical isolation.

5.1.7 Safety-critical redundant subsystems will be separated by the maximum practical distance or otherwise protected to ensure that an unexpected event that damages one is not likely to prevent the others from performing the function.

5.1.8 Safety-critical redundant subsystems will use dissimilar design to the extent practicable.

Rationale: Physical separation of safety-critical redundant subsystems is always desirable but not necessarily practical in areas of a spacecraft, e.g., system tunnels and engine compartments; therefore, other means, such as an overbraid, will be provided in certain instances.

5.1.9 Maintainability, accessibility, inspectability, testability, and the ability to detect performance degradations related to electromagnetic environmental effects will be demonstrated through the flight vehicle design life cycle.

Rationale: The flight vehicle design will be viable for electromagnetic environmental effects throughout the system's life cycle. This requires awareness, for example, of component aging characteristics, proper application of corrosion control and electrical bonding provisions that do not degrade, and a consideration of exposure of electronics to external electromagnetic environments when access panels are open. While advanced electronics and structural concepts offer advantages in increased performance of high-technology systems, these can be seriously compromised if electromagnetic compatibility design concepts impact life-cycle costs through excessive parts count, mandatory maintenance, or costly repair requirements to offset degradations.

5.1.10 Flight vehicle design safety-critical and mission-critical system functions will demonstrate a positive performance margin against electromagnetic effects at design end of life. This margin is typically 6 dB but may be tailored to suit the mission type.

5.1.11 Pyrotechnic devices and circuits will be designed and integrated so that induced electrical noise currents will be 16.5 dB below the device Maximum No-Fire Stimulus rating throughout the device life cycle.

Rationale: Electromagnetic effects margins should be included in the flight vehicle design to account for variability that will stem from differences in cable harness routing and buildup properties, quality of cable shield terminations, electrical bonding life-cycle adequacy, electronic component differences, and component degradation with aging and maintenance. In addition, uncertainties in the verification process may exist because of the verification method employed, limitations in environment simulation, and repeatability/accuracy of measured data. The proper application of margins in system and subsystem design provides confidence that the flight vehicle design will perform satisfactorily in the operational electromagnetic environments, in spite of these constraints and degradations.

5.1.12 The flight vehicle hardware required to operate during mission ascent/descent or during a depressurization or repressurization event, whether in sealed or unsealed enclosures, will be designed to prevent corona or arcing events from occurring.

Rationale: The electrical voltage required to initiate an arc across a gap between closely spaced conductors is a function of the ambient gas pressure, gap distance, and applied voltage. The voltage necessary to arc across the gap decreases as the pressure is reduced to a certain point, then increases, gradually exceeding its original value. Corona/arcing can cause EMI problems and/or contribute to hardware failures. Electrical/electronic components using a sealed chassis design that are powered only in pressurized conditions do not require corona/arcing testing.

5.1.13 Electronic equipment will be designed and integrated in the flight vehicle design to control emissions of and susceptibility to EMI.

Rationale: Electromagnetic emission and susceptibility characteristics of flight vehicle design equipment and subsystems should be controlled to obtain a high degree of assurance that these items will function in their intended installations without unintentional EMI with other equipment, subsystems, or external environments. The electromagnetic environment to be considered within flight vehicle design is complex and highly variable depending upon the various operating modes of the on-board equipment. Some of the primary factors driving the need for EMI controls are the presence of sensitive antennas and their connected receivers, which respond to interference generated within their intended tuning ranges, and the RF *emissions generated by on-board and external transmitters, natural and triggered lightning, and power supply components.*

5.1.14 Access to test ports for planned programming of reconfigurable devices will not require disassembly other than removal of standard connector caps.

Rationale: The greater the amounts of physical change to the box, the greater the inherent risk of introducing a failure or exceeding life limits on mechanical hardware. In addition, more extensive physical changes may require repetitions of any previously conducted physical acceptance test, such as vibration, bonding, etc.

5.1.15 GSE temperature gages, pressure gages, electrical meters, and similar readout devices will indicate normal system operating range in an easily recognized manner.

Rationale: This allows the operator to more readily detect/notice an out-of-range condition and ensures the readout device will adequately cover the operating range. For example, normal operating range on a gage should be in the center of the gage with marks that indicate minimum and maximum tolerance. The display should be in the correct units (English or metric).

5.1.16 Breakout boxes should be built for every connector that interfaces with flight hardware.

Rationale: Breakout boxes can help determine if the fault is in the cable or the test equipment or the flight hardware without opening any boxes.

5.1.17 Designers should balance operations characteristics (manufacturing, procurement, test, logistics, ground operations, flight operations, and facility design and vehicle design requirements), performance, and life-cycle cost during the design of components, systems, and subsystems.

Rationale: To successfully reduce production and operations costs, operations-driven hardware design is required beginning in the conceptual phase of design.

5.1.18 Flight hardware will be designed to support its own weight in the horizontal lifting and transportation configuration.

Rationale: This eliminates the need for expensive GSE to be designed to provide structural support for the flight hardware during ground operations.

5.1.19 Hazard detection and warning systems will be powered from an independent equipment or facility power bus.

Rationale: This prevents the common cause failure mode of power loss taking out the function and the ability to detect the loss of function, which would prevent corrective/mitigating action from being taken.

5.1.20 Flight hardware and software will be designed to facilitate ground and on-orbit maintenance and checkout activities and will be compatible with ground maintenance capabilities.

Rationale: Reliability analysis, Failure Modes Effects Analysis (FMEA), and heritage allows forecasting the most likely failures for each environment and use in which the system must operate. Building in preventive and corrective maintenance capability helps ensure mission success and the achievement of the required system readiness and launch availability.

5.1.21 The flight hardware will meet its requirements during and after exposure to its combined induced and natural environments during each mission phase (prelaunch, lift-off, ascent, stage separation, and stage re-entry, if recovered).

Rationale: Induced environments can degrade system performance, shorten system life, and lead to system or mission failure if not properly considered in the design. This is amplified when combined with natural environments.

5.1.22 Reliability/risk improvements expected from contingency capabilities will be quantified, including the estimated uncertainties, before committing to implementation.

Rationale: Often, the need for contingency capabilities is accepted because it is possible to add these capabilities without showing that there is a true benefit. Some examples from Constellation where contingency capabilities were included or recommended include manual steering, changing guidance targets in flight, and replacing navigation states. Issues that were not sufficiently examined include: the likelihood that the scenarios being addressed by contingencies might occur; the increased risk associated with the contingency from added complexity and decision making; and the risk from expending resources on contingency work, rather than covering nominal dispersed flight engineering and more likely scenarios.

5.1.23 All qualification components will be built to released engineering drawings.

5.1.24 All flight components will undergo a formal acceptance test program that includes performance testing.

5.1.25 Parts exposed to any concentration level of fluid media will be fabricated from materials that meet fluid compatibility requirements as indicated by an acceptable rating in the Materials and Processes Technical Information System (MAPTIS) in the worst-case usage environment and that have been assessed for the given fluid media.

Rationale: Aerospace fluids, especially those valuable in propulsion systems, are compatible with some materials but incompatible with others. For example, nickel-rich alloys, such as Monel®, are the preferred materials for use in contact with the oxidizer fluid in propulsion systems. However, nickel-rich alloys are highly incompatible with hydrazine, a common fuel in propulsion systems

5.1.26 Ground handling and transportation systems will be designed to the limit load accelerations of table 1 in ES22 Memorandum, Transportation and Handling Limit Load Factors.* As a general rule, it is recommended that ground handling and transportation system loads do not impose loads on the flight hardware that exceed the flight hardware design limit loads.

*NOTE: Copies available from ES/MSFC Thermal & Mechanical Analysis Branch.

Rationale: This principle establishes minimum design standards necessary for the ground handling and transportation system loads and environment to ensure that ground handling and transportation systems do not design the hardware. If needed, operation procedures and/or isolation systems can be employed.

5.1.27 The design will not use electrical connectors that require a blind mating in system-level assembly, test, and launch operations.

5.1.28 Use of mercury in components is to be avoided, when possible.

Rationale: Mercury is poisonous, a conductor that can cause shorts and structural failure of some materials. It is a liquid, migrates easily, and can vaporize. As a result, it is particularly hard to control. Mercury can also embrittle structural materials; therefore, its use in inspection devices, e.g., ultraviolet (UV) lamps and switches, used around flight hardware should be controlled.

5.1.29 Space-flight programs are to document how materials and processes will be selected, controlled, and implemented. An identification of the materials used and any variations for usage of materials are to be documented. In addition, controls for contamination concerns, foreign object debris concerns, and planned approaches for nondestructive evaluation (NDE) are to be documented. Methods to control red plague (cuprous/cupric oxide corrosion) and to maintain lead-free electrical hardware are also to be documented.

Rationale: Development and implementation of these elements provides assurance of appropriate materials and processes (M&P) selection, control, characterization, and usage to mitigate the risk of component and systems failure and that space-flight hardware is produced with the capability necessary to achieve mission success. For example, the Launch Abort System failures of two high-thrust sub-scale static test firings have been attributed to poor materials selection and use of poorly characterized materials for the design conditions.

5.1.30 Equipment using rotating mechanisms will incorporate provisions for containment of failed parts.

Rationale: Rotating equipment failure has many failure causes, e.g., structural or over-speed causes, which can throw high-energy shrapnel randomly, causing cascading failures or a direct hazard.

5.1.31 Containers, such as film containers, which may be pressurized with inert gas, will have a method of indicating positive pressure.

Rationale: This prevents a personnel hazard during opening of the container or over pressurization during filling.

5.1.32 Flight vehicle RF equipment will be designed and integrated to protect personnel, fuels, and electrically initiated pyrotechnic devices and circuitry against hazards from the effects of electromagnetic radiation during ground and flight mission modes.

Rationale: High-level electromagnetic fields can harm personnel, ignite fuel, and fire electrically initiated devices. If personnel have access to hazardous areas, appropriate measures will be taken, such as warning signs and precautions in written guidance and instructions. RF energy can induce currents to flow in any conductive object. The amount of current, and thus the strength of an arc or spark produced between two electrical conductors (or heating of small filaments), depends on both the field intensity of the RF energy and how well the conducting elements act as a receiving antenna: the main factors are the conductor length in relation to the wavelength of the RF energy and the orientation in the radiated field. Because it is not feasible to predict or control these factors, the hazard criteria will be based on the assumption that an ideal receiving antenna could be inadvertently created with the conductors. Restrictions on use of some RF emitters (power, frequency, separation distance) may be necessary to ensure safety *under certain operations, e.g., refueling or maintenance operations in which critical components are exposed.*

5.1.32.1 RF equipment will be shielded to prevent personnel exposure to RF levels greater than 10 mW/cm^2, except in front of the antenna.

Rationale: This prevents personnel from being radiated constantly when operating the equipment while not positioned in front of the antenna.

5.1.32.2 System designs will preclude the generation of sound pressure levels above 85.0 dB(A).

Rationale: This prevents operators and maintainers from being exposed to harmful or permanent hearing damage.

5.1.33 Radioactive materials will not be used for any purpose, unless it can be proven that a non-radioactive substitute material cannot be used.

Note: See NPR 8715.3, NASA General Safety Program Requirements, for the processes to be used for radioactive material usage.

Rationale: This prevents personnel exposure to radiation and eliminates the complex methods of control that are required for radioactive materials.

5.1.34 The flight vehicle design will provide verifiable low-resistance electrical bonding mechanical interfaces between vehicle structural and outer surface components and internal components for control of environmental lightning currents, vehicle power supply fault currents, and electrical interference noise currents, so that the flight vehicle design operational performance requirements are met.

Rationale: Good electrical bonding practice is a key element of a successful flight vehicle system design, which generally includes the use of ground planes to form equipotential surfaces for circuitry. If voltage potentials appear between electronics enclosures and the ground plane related to internal circuitry operation, the enclosure will radiate interference. Similarly, electromagnetic fields will induce voltage potentials between poorly bonded enclosures and the ground plane. These potentials are imposed as common-mode signals on circuitry referenced to the enclosure. The same two effects will occur for poorly bonded cable shield terminations. Bonding provisions help control voltage drops in power current return and fault paths, and without proper bonding, lightning interaction with the flight vehicle design can produce voltages that can shock personnel, ignite fuel through arcing and sparking, ignite or dud ordnance, and upset or damage electronics. As electrical bonding involves obtaining good electrical contact *between metallic surfaces while corrosion control measures often strive to avoid electrical continuity between dissimilar materials, it is essential that the requirements of each discipline, though potentially conflicting, be fully considered in the flight vehicle design.*

5.1.35 Flexible hoses will have a minimum slack allowance of 5 percent of the total hose length.

Rationale: This allows for expansion/contraction, prevents excessive stress, and allows for unknowns in the system, such as distance between couplings.

5.1.36 Shut-off valves will not be installed in series with relief valves unless another independently operated positive relief device is installed in parallel with the shut-off valve.

Rationale: This prevents disabling of the relief capability.

5.1.37 Design for Manufacturing

5.1.37.1 Space-flight hardware designs, including test articles, will be evaluated for efficient manufacturing by integrated product and lean manufacturing teams that include responsible Engineering Department (Design, M&P, Test, etc.,) organizations.

Rationale: Efficient manufacturing activities have a direct impact on the ability to reduce schedule time and resources required, which results in an overall life-cycle cost savings to the program.

5.1.37.2 Fabrication and assembly operations will be evaluated for the following:

a. Critical stress conditions from materials handling.

b. Forming, stretching, or other processing.

c. Clamping, misfit, and misalignments.

d. Welding and re-welding.

e. Heat treatment.

f. Bonding.

g. Brazing.

h. Coating.

i. Sequencing of contamination-generating operations before final cleaning when possible.

j. Factory checkout and acceptance operations, including pressurization cycles.

5.1.37.3 Designs will establish the critical data for manufacturability no later than PDR.

Rationale: Examples of critical data include interface locations, weld land widths, and critical inner and outer mold line dimensions. These dimensions can be contained in a simplified model of the assembly, without detailed design information, but will be controlled at a project or chief engineer level, because of the enormous budget and schedule impacts resulting from their change.

For example, this principle is critical to the NASA systems engineering approach. It allows the long-lead tooling acquisition and helps define any manufacturing scale-up test article dimensions. As an example, Ares I Upper Stage common bulkhead domes required more than 1 year to produce spin-form tooling, which was needed early in the program to retire manufacturing risk. The designers provided an early version of the design so tooling could be ordered and the project schedule could be preserved. Subsequent detailed design changes were reflected by change orders to the tooling design.

5.1.38 Sealing plugs will be placed behind unwired contacts.

Rationale: Without sealing plugs, an environmental connector will not be sealed from its external environment.

5.1.39 Connector and cabling will include design features that preclude inadvertent connector mating.

Rationale: Connectors in close proximity to each other and having the same or similar insert arrangements are subject to mismating, which may cause circuit damage, unintended operation, and/or failure. Connectors will be chosen to preclude mismating by the appropriate selection of insert arrangement, shell size, clocking, etc. Labelling is insufficient for error protection.

5.1.40 Removable contacts on connectors will be retention tested.

Rationale: Removable contacts that become disengaged may become contamination debris.

5.1.41 Unmated connectors will have mating surfaces protected by covers during storage, handling, installation of harness, and ground operations and flight.

Rationale: Protective covers prevent contamination.

5.1.42 Unused contact cavities on a connector will be populated with unwired contacts.

5.2 Aero Sciences

Content will be added to this section in the future.

5.3 Electrical Power

5.3.1 EEE parts obsolescence management and control will meet the requirements of MSFC-STD-3620, MSFC Electrical, Electronic, Electromechanical (EEE) Parts Obsolescence Management and Control Requirements.

5.3.2 The flight vehicle design electrical systems will incorporate a distributed single-point ground power and signal grounding architecture.

Rationale: An electrical system, such as that in the flight vehicle design, is grounded for three reasons: safety, enhanced operability of the circuit, and EMI control. Some electrical circuits require grounding to a common reference plane (ground plane) to operate efficiently. A single reference to structure prevents unwanted direct current (dc) and RF noise currents from circulating through structure, thereby mitigating potential EMI problems. To establish a distributed single-point ground reference for the flight vehicle electrical power system, it is necessary to define isolation requirements at equipment interfaces. It is also necessary to ensure that secondary electrical power systems and electrical signals routed externally to equipment meet the isolation requirements to prevent multiple signal references to structure (ground loops).

5.3.3 To ensure maximum compatibility among the various worldwide users of the electromagnetic spectrum, it is essential that antenna-connected equipment used in NASA projects and programs comply with established Federal spectrum usage and management requirements. Spectrum planning and frequency management should be given appropriate and timely consideration during the development, procurement, and operation of flight vehicle designs that use the electromagnetic spectrum.

5.3.4 Powered-off electronic circuits will not be damaged by the application of nominal signals to their inputs and nominal loads to their outputs.

Rationale: This capability eliminates power sequencing problems and aids in prevention of fault propagation.

5.3.5 Digital circuit designs will initialize into a known state.

Rationale: Fundamental aspects of digital circuit design will be implemented for designs to be sufficiently robust for reliable operation.

5.4 Fault Management

5.4.1 The fault management system design will detect critical function failures as defined by hazard analyses and critical faults as defined by FMEAs that affect mission objectives or crew safety to support successful failure response.

Rationale: Detection of critical function failure and critical faults enables crew, ground, mission support personnel, and automated systems to respond as appropriate to maintain vehicle performance and mission success where possible and to ensure crew safety. These responses include goal changes, e.g., aborts, recovery actions, e.g., redundancy management, and masking. Hazard analysis reports define multiple, non-coincident faults. FMEAs define single faults and common cause failures. The program will determine, through analysis, the failures that require detection and the associated methods for detection. The effectiveness of failure detection is based on analysis of true positive/false positive/false negative for the detection mechanisms. For example, the Space Launch System (SLS) uses an approach called the Goal Function Tree, which integrates these methods.

5.4.2 The fault management will be designed to provide a safety net of failure detections and responses that protect the system's highest level goals, independent of quantitative risk assessments. These should be designed to provide a near-guarantee to detect threats to the system's goals, though it may not be feasible to ensure sufficient response time in all cases.

Rationale: It is impossible to guarantee that system designers and operators will be able to foresee all possible causes of failure. Thus, some last-ditch detection and response capability needs to be provided that protects the system's most important goals and assets, regardless of the cause of failure and regardless of the quantitative estimates of failures and risks. The safety net is a protection against "unknown unknowns" and is based on "possibility," not "probability." It should be designed based on detecting compromises to achieving the system's *goals as specified in success space, not failure space, since it is much easier to determine what the system must do and hence detect that it is not doing what was intended, as opposed to trying to predict all the ways the system might fail.*

5.4.3 The fault management system design will detect multiple, non-coincident faults, provided that they occur in independent fault containment regions.

Rationale: Having dealt with prior faults, it is nonetheless important to preserve remaining options for mission success. The likelihood of faults in independent fault containment regions is undiminished. Coincident faults, however, are generally of sufficiently low likelihood to justify making no overt provisions for them in the design.

5.4.4 Fault management control loops (the entire chain from detection through response) will be designed to ensure they provide a significant reliability, availability, or safety benefit to the system. The benefits of fault management control loops are generally measured as reliability, availability, or safety or dependability metrics expressed in probabilistic terms and should be quantitatively specified as system-level requirements to improve system dependability.

Rationale: The value of fault management control loops can and should be estimated to ensure they are providing significant system benefits and justified on that basis. Requirements should be specified to identify the amount of reliability, availability, and/or safety improvements desired from the fault management system.

5.4.5 Fault management system failure detections will be designed so that the probability of false positive of these detections is at least two orders of magnitude below the reliability, availability, or safety benefit of the failure detection. False positive performance will be estimated and measured on a per-mission basis.

Rationale: False positives, the indication that failure has occurred when it has not, may lead to a loss of mission and should be reduced to ensure that the value of the failure detection is far greater than the decrease in that value because of the unreliability of the detection. Since detection of failures is a function distributed across the vehicle elements, a vehicle requirement is necessary to establish the acceptable limits in falsely indicating that a failure has occurred.

5.4.6 The fault management system design will qualify data from sensors that are used for vehicle control or failure detection.

Rationale: Sensor data are analyzed by predefined criteria to distinguish between data that accurately represent the state of the system, i.e., qualified, and data that have been corrupted by *a sensor, data path, or other failure to ensure that data acquired from flight-critical sensors are valid before use in vehicle control or failure detection algorithms.*

5.4.7 The fault management system design will detect anomalies for all mission phases.

Rationale: There is no performance requirement on anomaly detection, because, by definition, anomalies are unexpected. Anomaly detection is generally based on expert knowledge of system behaviors and, if automated, through training-based systems. For prelaunch or long-duration in-flight anomalies, detection can be in real time or after the mission. For short-duration missions, anomaly detection can occur after the mission.

5.4.8 The fault management system design will isolate critical faults as defined by FMEAs and failures of critical functions as defined by hazard analysis to the level identified in table II, Fault Isolation per Mission Phase, to support mission objectives and crew safety

Table II. Failure Isolation per Mission Phase

Mission Phase	Isolation Level
Preflight	LRU level for repair or replace
Short-Duration In-Flight	Level necessary to execute proper response action
Long-Duration In-Flight	LRU level to execute proper response action to pre-empt failure
Postflight	Level necessary to support future missions or design changes

Rationale: The specific amount of time allowed for isolation (determination of the location of a fault) is based on the system availability requirements for prelaunch and for in-flight system reliability requirements. Postflight fault isolation should be performed in time to support the next mission. Isolation performance is based on analysis of true positive/false positive/false negative for the isolation mechanisms.

5.4.9 The fault management system design will isolate multiple, non-coincident faults, provided that they occur in independent fault containment regions.

Rationale: Having dealt with prior faults, it is nonetheless important to preserve remaining options for mission success. The likelihood of faults in independent fault containment regions is undiminished. Coincident faults, however, are generally of sufficiently low likelihood to justify making no overt provisions for them in the design.

5.4.10 The fault management system design will respond to failures of critical functions as defined by hazard analysis and critical faults as defined by FMEAs that threaten mission objectives and human safety.

Rationale: This is a system-level requirement for which vehicle, ground, software, and operations requirements are derived. The specific amount of time allowed for failure response and the effectiveness of that response is based on the system availability requirements. Response effectiveness is based on analysis of the race condition of the time to criticality versus the fault management control loop that is mitigating the failure (including detection, isolation, and response) and also an analysis of the interactions of the response with other system control loops, including nominal control loops and fault management control loops. The failure response types are failure goal change, failure recovery, failure masking, and operational failure avoidance. For in-flight responses, goal change generally includes abort for crewed vehicles and safing generally; failure recovery includes fault detection, isolation, and response and redundancy management in which the failure temporarily compromises a function but not a system objective; failure masking typically includes voting mechanisms for computer and control system redundancy management such that the function is not compromised; operational failure avoidance usually exists only for long-duration or reusable vehicle missions and includes failure prognostics (often based on trend analysis) to predict when a failure will occur and making changes to flight sequencing or repairing or replacing components in flight (for long-duration crewed vehicles) or between flights (for reusable vehicles).

5.4.11 The fault management system design will respond to multiple, non-coincident faults, provided that they occur in independent fault containment regions.

Rationale: Having dealt with prior faults, it is nonetheless important to preserve remaining options for mission success. The likelihood of faults in independent fault containment regions is undiminished. Coincident faults, however, are generally of sufficiently low likelihood to justify making no overt provisions for them in the design.

5.4.12 The system will provide notification of critical failure conditions to support failure response decisions.

Rationale: This is a general principle to provide information to the portions of the system that are involved in failure response, whether automated or human in the loop. It is essential for the system to provide sufficient data for humans to have current situational awareness of system failure conditions and for the data to be provided in a timely manner to enable human response. Notification is defined as delivery of interpreted information to the user of this information, in this case, the person or machine responding to the failure.

5.4.13 The system will provide notification regarding actions taken in response to failures.

Rationale: The system is known by test to be in a stable, safe, sustainable configuration following fault protection activation. Commanding is not needed, nor should it be initiated until a complete understanding of the events and thorough recovery strategy have been established, since more harm than good could result. This approach depends on receipt of the fault protection response telemetry.

5.4.14 The fault management system design will respond to time-critical failures that threaten humans or critical functions without the need for external intervention. Acceptable responses to critical failures are recovery, abort, and safing.

Rationale: This is a general principle to provide for autonomous response by the system in situations where there is a loss of communications or where a low time to criticality precludes a timely response by the crew. This principle applies to both prelaunch and in-flight time-critical failures.

5.4.15 For long-duration missions, the system will predict the time of future critical, slow time-to-criticality failures, so as to enable successful action to prevent the future failures.

Rationale: This principle applies only to long-duration missions (generally, several hours at minimum). Today, the failure prognosis function is usually ground based, though some capability could be based on board. Missions extending farther than 3 light minutes from Earth will require this capability on board to protect the crew. Wherever it is located, the function will provide predictions quickly and accurately enough to enable successful operational failure avoidance actions. The predictive capability is the anticipation of the consequences of the trend of current vehicle behaviors. If the future consequence of current behavior is failure, then actions should be taken to prevent or mitigate the consequences of that failure.

5.4.16 The fault management system design will provide the data necessary to diagnose failures.

Rationale: It is essential for the system to provide sufficient data to enable failure diagnosis and to enable reconstruction of failures, so that the initiating event(s) can be identified and the root cause can be isolated.

5.4.17 The fault management system will provide the ability to maintain the vehicle in an operational state, when possible, to improve mission success.

5.5 Flight Mechanisms

Content will be added to this section in the future.

5.6 Guidance, Navigation, and Control

Content will be added to this section in the future.

5.7 Human Systems Integration

5.7.1 Launch system, payloads, spacecraft, and test systems design will perform usability assessment for all human/machine interfaces for human or robotic systems:

a. Assembly/disassembly, handling, and transportation.

b. Testing and troubleshooting, including alignments, and calibrations.

c. Maintenance and servicing in the planned ground operations flow, including integrated operations with the launch vehicle.

d. On-orbit assembly, integration, and maintenance.

5.7.2 The design will provide positive clearances to contacting surfaces for all separations, deployments, releases, jettisons, and articulations under nominal and 3-sigma worst-case conditions.

5.7.3 Systems will be designed so that it is physically impossible to install components in reverse.

Rationale: This requirement prevents a failure mode that has been catastrophic in the past. Human error is a leading cause of failure and can become a common cause of failure if the same person installs all the redundant systems in the same way but incorrectly. This does not apply to the design of subsystems, i.e., printed circuit boards.

5.7.4 Human systems integration principles will be applied to all system design.

Rationale: Application of the human systems integration principles and processes through design and development will assure that functions are properly allocated between humans and machines and that human tasks performed by NASA, whether during ground operations or in *flight, can be performed with minimal risk to flight systems. The principles and processes are defined in a Human Systems Integration Plan appropriate to the project or program.*

5.7.5 Human factors and operations engineering will evaluate the design and packaging of internal flight hardware to ensure supportability, maintainability, and GSE functionality and interface.

Rationale: Human factors and operations engineering analyzes the design for maintainability and supportability human touch tasks. These analyses may identify location of enhancing access and operability for servicing LRU/Orbital Replacement Unit (ORU) replacement.

5.8 Materials, Processes, and Manufacturing

5.8.1 General

Note: A unique resource for M&P data for the aerospace community is MAPTIS, http://maptis.nasa.gov/home.aspx database, retrieved 8-28-14.

5.8.1.1 The Material Readiness Level (MRL), Process Readiness Level (PRL), and Technology Readiness Level (TRL) of materials and manufacturing processes selected will be commensurate with the phase of the design/development to avoid unnecessary risk, additional development costs, and potential schedule impacts.

Rationale: Materials, Processes, and Manufacturing engineers should make sure that the technologies used by the project/program are sufficiently mature and do not pose a significant risk to the project. For example, materials and processes selected for design should have an MRL, PRL, or TRL of 6 or greater at CDR.

At MRL 6, material is available and used in components acceptable for flight. At PRL 6, the process applied to an object has produced defect-free flight acceptable components, process parameter ranges are identified, and integration and operations procedures are partially developed. At TRL 6, the system/subsystem model or prototype has been demonstrated in the relevant environment (ground or space).

5.8.1.2 A material or process with an MRL, PRL, or TRL below 6 should not be chosen for a design since it has not been matured or tested to have sufficient readiness.

Rationale: Inadequately characterized materials and manufacturing processes can pose significant risks to a project. For example, the External Tank (ET)/Super Light-Weight Tank specified a weld filler alloy that was inadequately characterized, resulting in extensive cracking.

This choice necessitated a change in filler alloy, resulting in significant cost and schedule impacts.

5.8.1.3 Materials selection will include evaluation of long-term availability, obsolescence, and environmental impact issues to minimize risk of costly redesign.

Rationale: Materials selection includes not only structural materials but also chemicals used during manufacturing processes. Changes in Environmental Protection Agency and Occupational Health and Safety Administration regulations and the commercial market may have an impact on the availability of materials and solvents used for fabrication and manufacturing. Materials that become unavailable or in short supply because of obsolescence or updated environmental regulations may increase costs for procurement. Requalification of flight hardware produced with replacement materials is likely to increase cost. Replacement materials may also require changes to production sequencing and tooling, which may impact both cost and schedules. Failure to anticipate and plan for such shortages may result in production stoppages with significant impact to both cost and schedules.

5.8.1.4 Hardware designs will consider adequate controls over materials, manufacturing processes, packaging, transportation, test, operational processes, and exposure or use environments to help ensure process repeatability, as well as product functionality, consistency, and optimum reliability.

Rationale: There is a history of program and project insufficient funding to support adequate M&P insight activities during the hardware development phase. Programs typically assume increased risks related to inadequate material selection, material control, and process control. Small changes in vendor formulations, material content, or processing are often discovered only after a failure or reduction in a component's performance.

5.8.1.5 In cases in which designs will eventually lead to production processing, designers will support lean manufacturing events conducted by manufacturing personnel.

Rationale: These events are conducted to ensure that the design concepts can be manufactured in a cost-effective and efficient manner.

5.8.1.6 Design will take into consideration manufacturing and processing limitations of the materials being used.

Rationale: Composite materials, adhesives, and sealants can be sensitive to the time required to form the part, between removing material from the freezer and before curing begins.

5.8.2 Material Characteristics

5.8.2.1 Materials will be characterized to permit reliable and high-confidence predictions of their properties: general physical properties, including thermal characteristics; allowable mechanical properties; fracture properties (if fracture critical or if properties are needed for assessment to classify as non-fracture critical); material failure mechanisms; age life properties; and compatibility (interactions of surrounding materials/processes).

Note: Age life is a portion of characterization of new or modified materials, and compatibility is often overlooked when selecting a material. For example, thermal protection system (TPS) evaluations may need to be conducted for every substrate over which the TPS is used and with which it may come in contact during processing to include (but not limited to) solvents used to clean the substrates.

Rationale: Poor materials characterization and selection may result in component or systems failure. For example, testing for the SLS Multi-purpose Crew Vehicle Launch Abort System resulted in high-thrust test failures, which have been attributed to poor materials selection and use of poorly characterized materials for the intended design requirements.

5.8.2.2 The M&P Laboratory will determine the values of knockdown factors to be used on design material properties.

Rationale: The effect of variation in material properties related to processing of the material and subsequent manufacturing processes, including considerations such as exposure environment and temperature, is usually accounted for in the property values provided to the design organization. Any further reduction in properties should be coordinated with M&P to avoid redundant knockdowns and could result in an overly conservative design.

5.8.2.3 Technical rationale for setting design strength values equal to lot acceptance requirement values will be provided when defining design properties for metallic materials.

Rationale: Certain alloys and product forms exhibit a difference between statistical design strength and lot acceptance values. This can result in design values that are not protected by the lot acceptance test. Setting strength design values equal to lot acceptance requirement values is a safe practice with common aerospace materials that have a long production history. However, custom alloys and product forms, e.g., spin-formed products or thick plate, that are not covered in United States agency-approved specifications or handbooks, e.g., NASA, Department of Defense, Federal Aviation Administration (FAA); specialty alloys that are sensitive to small variations in elemental alloy content, e.g., low interstitial titanium (Ti) and aluminum-lithium;

and materials that have lot acceptance requirements on both strength and fracture toughness, e.g., aluminum-lithium and some rolled ring forgings, may exhibit lot-to-lot variation to the extent that the statistically based design allowable for the alloy is below the lot acceptance value for the material. This happens when the actual lot acceptance test values begin to consistently approach the minimum lot acceptance requirement. It is important to identify the potential for this type of behavior in an alloy and to evaluate the related system level risk. To assess the potential for this type of behavior, historical trends in the lot acceptance test data should be reviewed. In cases where lot acceptance values are trending downward or exhibit a large amount of variability, a process control review team should be established to monitor trends in lot acceptance behavior as material continues to be purchased. For example, a review of historical lot acceptance data from a vendor producing aluminum-lithium material revealed that, although all of the material met the minimum lot acceptance requirements, the statistically based design allowable calculated from the test data was approximately 2 percent below the lot acceptance value. Risk associated with this behavior was addressed in the contract end-item specification.

5.8.3 Fracture Control

5.8.3.1 Fracture control is to be implemented on manned space-flight programs to mitigate the risk of catastrophic failure related to crack-like defects, flaws, or impact damage to composite or bonded hardware. Fracture control may also be implemented on unmanned programs to enhance mission reliability by reducing the risk of catastrophic failure.

Note: Fracture control requires that all manned space-flight hardware be assessed to determine if structural failure of the part related to a flaw would result in a catastrophic failure. If the assessment determines that failure of the part, because of a crack-like defect or damage site (composite materials), would result in a catastrophic failure, then that part is fracture critical, unless specifically verified to satisfy one of the non-fracture critical categories (or an acceptable approach) contained in NASA-STD-5019, Fracture Control Requirements for Spaceflight Hardware. Fracture control requirements and criteria exist to promote safety during manned spaceflight. Fracture-critical parts receive additional risk mitigation activities, including activities to understand defect sensitivity of the part, e.g., fracture analysis, damage tolerance test, proof test; activities to understand if any defects exist in the part, e.g., NDE, proof test, process control; implementation of adequate materials and processes in part design and usage; and activities to provide traceability of materials, loads, handling, and usage.

Rationale: Fracture control practices represent a design for minimum risk approach for manned flight programs. Awareness of the fracture control process is necessary to minimize either increased risk during flight or unplanned implementation costs during design.

5.8.3.2 Use of Ti alloys at temperatures below -101 °C (-150 °F) will require damage tolerance characterization, e.g., determine fracture properties (fracture toughness ($K_{1c)}$; crack extension per cycle (da/dN), service life, etc.

Rationale: Ti alloys exhibit a significant increase in strength and a significant decrease in fracture toughness as operating environments approach cryogenic temperatures. This results in diminishing critical flaw sizes that can easily fall below reliable NDE detection sizes. As an example, feedline brackets for the ET were redesigned using Ti to decrease potential for ice buildup and minimize the use of thermal protection materials. However, because of the proximity of the brackets to the liquid oxygen tank, the design service temperature was -250 °F. Testing at the service temperature revealed a drop in fracture toughness of 25 percent below the room temperature values. A robust design (large safety margins) was maintained in the bracket to ensure critical flaw sizes remained above NDE detection capability.

5.8.4 Structural Materials

5.8.4.1 Values for design mechanical properties for structural materials, e.g., metallic, composite, ceramic, additively manufactured, or structural joints, e.g., welded, brazed, adhesively bonded, diffusion bonded, are to be evaluated with respect to their specific operating environment. Design properties not provided in standard sources such as the Metallic Materials Properties Development and Standardization (MMPDS) or CMH-17, Composite Materials Handbook, are to be based on test data generated in the operating environment, and design properties should be determined by statistical approaches in accordance with the MMPDS or CMH-17.

Rationale: The basis for design mechanical properties in their specific operating environments should be developed and documented to mitigate risk of failure associated with structural materials. For example, many metallic alloys are susceptible to hydrogen environment embrittlement that can result in strength capability that is a fraction of the strength capability in a non-hydrogen environment.

5.8.4.2 MMPDS material allowable A values will be used whenever failure of a single load path would result in loss of structural integrity. MMPDS material allowable B values may be used in redundant structure in which the failure of a component would result in a safe redistribution of applied loads to other load-carrying members.

5.8.4.3 Load-carrying structural composites will be assessed as described in MSFC-RQMT-3479, Fracture Control Requirements for Composite and Bonded Vehicle and Payload

Structures. If a damage tolerance approach is chosen, then a statistically based damage tolerance allowable will be developed in lieu of pristine material allowables.

Rationale: Assessment of capability for composites with impact damage or manufacturing flaws is a bounding approach to assessment of pristine (undamaged or unflawed) composites.

5.8.4.4 Use of aluminum alloys in plates over 3 in thick requires characterization of short transverse (S-T) properties.

Rationale: Although thick-plate aluminum alloys exhibit good properties in the longitudinal and longitudinal-transverse directions, there are concerns with properties in the S-T direction that are not identified in the aerospace specifications or MMPDS. Thick-plate aluminum can exhibit low ductility and sometimes completely brittle behavior in the S-T direction. This can become an issue when thick-plate material is used in machining brackets and other support/connection structure with complex geometries and result in hardware with principal stresses oriented along the S-T direction or other directions outside the rolling plane of the material. For example, MSFC generated a limited data set on thick plate (5 in) proposed for use in fabricating brackets for use in the International Space Station (ISS) pressurized mating adaptor (PMA). The testing revealed S-T ductility as low as 0.6 percent. Based on the test results, the material was rejected for use in the PMA since the bracket would see high loads in the S-T direction. Additionally, MSFC M&P generated test data for 2219-T87 thick plate, purchased in accordance with specification requirements. Total elongation in the S-T direction ranged from 0.66 to 0.92 percent (eight specimens over two heat lots). The data reflected low values for elongation in the S-T direction and a high degree of variability in elongation within a given plate.

5.8.4.5 Special care should be taken when using aluminum-lithium alloys, specifically on the appropriate failure criterion to use when assessing margins of safety for yielding of the aluminum-lithium components or structures.

Rationale: Yield behavior for aluminum-lithium alloys may not follow the von Mises yield criterion commonly used for ductile metals. Yield stress margins are often based on effective stress levels versus an allowable uniaxial yield strength. Because of the strong texturing and anisotropic behavior that can be present in aluminum-lithium alloys, this may result in a non-conservative assessment of the yield margin. For example, recent testing on nominally 2-in thick aluminum-lithium plate under combined tension and shear revealed failures below the von Mises yield criterion prediction. The appropriate failure criterion may vary, depending on the specific aluminum-lithium alloy, the product form, the product dimensions, the service temperatures, and the direction of predicted stresses relative to the material grain directions.

5.8.5 Age Life/Shelf Life/Traceability

For materials and components whose shelf life has expired, the material has not been opened/used, and there is a desire to use the material, using the same acceptance tests as determined by the engineering community will recertify the material. The material can be certified if it meets the acceptance test requirements. For critical materials, the material may not exceed the shelf life as tested in qualification. Shelf life extensions only apply to the unused material remaining in stock that has been properly stored.

Rationale: Shelf life time is the maximum period of time from formulation date to the date the product is used as a component part in subassemblies, assemblies, and systems. During the shelf life time period, the stored product is expected to retain its characteristics. Structural adhesives, TPS, and other critical items may only be used for the period of time for which they have been qualified. For example, Alliant Techsystems, Inc., had a stockpile of critical materials used for cleaning, bonding, and surface activation. Because of delays in the Shuttle manifest, the stockpiled material surpassed the manufacturer's expiration date. The material was tested to ensure that its chemical formulation and performance met the required specifications.

5.8.6 Material Combustion Hazards and Prevention

5.8.6.1 Materials used on NASA vehicles and in GSE should be nonflammable in their use conditions. Materials that are flammable require a Material Usage Agreement (MUA) explaining what application is acceptable.

a. These materials should not ignite.

b. If no material is available that will not ignite, then the selected material should cease to burn if it contacts an ignition source.

Rationale: Electrical wires within the systems sometimes short circuit or overload, which can give off sufficient heat to ignite a surrounding material. At other times, an equipment malfunction can emit an ember or spark onto a material. It is imperative to use materials that will not ignite or sustain burning because of these possibilities. For example, the Apollo 204 fire, which killed three astronauts, was caused by an electrical wire shortage that occurred after the module was filled with an oxygen-rich mixture. The shortage caused the wire insulation to ignite, which, in turn, ignited other materials.

5.8.6.2 Special precautions will be taken when dealing with all materials used in oxygen systems.

Rationale: Fires occur when a fuel, an oxidizer, and an ignition source are present. Oxygen systems are especially hazardous because oxygen is an oxidizer, and the fuels are the materials *from which the system is built, especially the polymer seals. Neither of these factors can be eliminated.*

5.8.6.3 Two design rules will be followed to ensure the safety of oxygen systems:

a. The most burn-resistant materials will be chosen.

Note: The best metallic materials are high nickel and high copper alloys. The most burn-resistant nonmetals are fluorine-rich materials, such as polytetrafluoroethylene.

b. The system will be designed to minimize the number and severity of ignition sources that exist within the system. Since it is virtually impossible to use all nonflammable materials in an oxygen system design, an Oxygen Hazard Analysis should always be performed~~.~~.

Rationale: Potential ignition sources for oxygen fires cannot all be eliminated from the system. For example, there is a potential for a substantial heat increase when an oxygen system is rapidly pressurized. Operating procedures should be written to ensure that all pressurization is performed slowly, but procedures are not always understood exactly. Also, most oxygen systems have valves that open and close. This motion and surface striking creates heat. If the valve is not designed or operated properly, then the heat generated by the valve is enough to create an ignition. For example, the Space Shuttle Extravehicular Mobility Unit, better known as the astronaut spacesuit, ignited during a test at Johnson Space Center (JSC). This suit was the selected design to be manufactured and worn by the Shuttle astronauts. A spacesuit was being tested on a laboratory table, and oxygen began to flow into the suit in the manner it would when an astronaut is wearing the suit in space. Suddenly, a flash fire occurred as the technicians were standing next to the suit. The fire resulted from high-pressure oxygen flowing into an aluminum regulator that unknowingly contained one or more ignition mechanisms.

5.8.6.3.1 Safety of Materials in Crew Areas

Additional safety precautions will be taken when using materials in the crew areas.

Rationale: Nonmetallic materials can offgas, a process of emitting gasses or chemical compounds into the surrounding air. Offgassing produces chemical compounds in the air that astronauts breathe and is a common characteristic of nonmetals. On Earth, the offgassed chemical compounds do not accumulate to a hazardous level because of adequate ventilation; however, no ventilation is possible on space vehicles. Chemical compounds are scrubbed from breathing air to prevent hazards to astronauts, but current scrubbers are unable to trap all chemical compounds that are produced. For example, an experiment designed by a university was scheduled to be installed on the ISS. The university experimenters did not know much about the requirements that NASA places on its flight materials and did not build the hardware with optimum materials. When the experiment was tested for toxic offgassing, a significant amount of *carcinogens was produced. Vehicle materials are not to offgas chemicals as hazardous as carcinogens.*

5.9 Mechanical Systems

5.9.1 The use of cadmium fasteners is not recommended for new designs. The approval process can be time consuming and problematic.

Rationale: Cadmium is one of those materials that the Government desires to regulate out of use because it is a carcinogen and is otherwise hazardous. It is still available as a coating in various fastener standards. Because of its adverse effects on human health and the environment, use and exposure to cadmium represent occupational safety and environmental risks. While cadmium-plated parts offer advantages such as stress corrosion resistance and torque control, they are susceptible to hydrogen embrittlement and sublimation in vacuum environment, and their use in crew environments is potentially hazardous. Some were used strategically on the ET; however, the cadmium plating process creates a toxic environmental threat. NASA, because of its heritage and emphasis on safety, prefers to not use them. There may be applications, as in the case of ET, where such fasteners win out.

5.9.2 Details on fastener installation will be provided on the drawing, e.g. preload torque, torque limits, sequences, etc.

5.9.3 Quick-release fasteners will be used where consistent with other requirements, e.g., strength, sealing.

5.9.4 Part numbers will be located so that they are visible and oriented in an appropriate direction for operations after assembly and integration.

Rationale: Part numbers that are not visible after assembly are unable to fulfill their function of identification. Barcodes or other automation aids have to be able to be read by the barcode reader, which may have clearance requirements.

5.10 Natural Environments

5.10.1 General

5.10.1.1 Design environment ranges will be based on acceptable risk and operational restrictions.

Rationale: For virtually any environment, the measured extremes are typically too severe and too infrequent in occurrence to account for them solely by design. For environments that are not observable on the day of operation and, thus, not avoidable by operational constraints, the design range is typically set from the 1st to the 99th percentile. One relies on design margin to mitigate the risk of environments outside this range. For observable environments, the range may be relaxed but typically not beyond the 5th to 95th percentile range. Otherwise, cumulative constraints make normal operations prohibitive.

5.10.1.2 Where possible, the natural environments will be specified with uncertainties and probabilities of occurrence but without adding margin.

Rationale: Specifying uncertainties, probabilities, or rates of occurrence enables understanding of integrated risks and operational constraints. To prevent double bookkeeping, all margins should be kept by the engineering function.

5.10.1.3 The program's systems engineering process will actively integrate natural environments to identify a cost-effective and technically sound balance between robust design and operational procedures and constraints.

Rationale: Generally, the most effective approach is a combination of robust design, operational constraint, and accepted risk. It is essential that the environment specifications be tailored to the specific mission (Design Reference Mission (DRM) or equivalent). Changes in key mission factors, such as orbit, duration, or objective, often have significant impact, for better or worse, on how environments affect the system development. Experience with past programs has shown that failure to properly address the natural environments early in the program has resulted in excessive schedule and cost impacts.

5.10.1.4 Confidence limits (implicit or explicit) for natural environment specifications will be commensurate with the risk to the vehicle.

Rationale: Uncertainties in environment models and data sets vary widely from environment to environment because of differences in difficulty of measurement, natural variability, and period of record. Likewise, the risk to the vehicle if the flight environment exceeds the specification varies greatly. Sound engineering practice demands these variables remain compatible.

5.10.1.5 Programs using probabilistic risk assessments (PRA) will allocate a portion of their failure numbers to natural environments by program System Definition Review (SDR).

Rationale: This is typically done for meteoroids/orbital debris and should also be done for environment-related failure modes as well. These allocations should be complete by program SDR so that design work can begin independent of the integrated risk analysis.

5.10.1.6 Natural environments will be included into the estimate of launch and landing availabilities.

Rationale: Knowledge of launch and landing availabilities is required to support management decisions on accepting additional launch and/or landing restrictions and to support logistics, launch and landing recovery operations planning, and life-cycle cost estimates. Natural environments play a key role in these availabilities, and previous programs have found that natural environments can drive these availabilities to undesirably low levels.

5.10.2 Terrestrial and Planetary Environments

Vehicle systems and subsystems will be designed to meet their reliability and performance requirements during and after exposure to the following:

a. Wind environments.

b. Atmospheric temperature, humidity, and air density.

c. Atmospheric electricity.

d. Solar/thermal/cosmic ray/energetic electrons/energetic protons radiation environments.

e. Atmospheric pressure environments.

f. Atmospheric constituents.

g. Precipitation environments (rain and snow).

h. Cloud (liquid and ice crystals).

i. Fog environments.

j. Flora and fauna environments.

k. Sea state environments.

l. Landing on defined surface characteristics and topography environments.

m. Before, during, and after exposure to Mars and other planetary environments that can include the atmosphere, the surface environments, and the environment of space (such as planetary orbit) near the planet.

5.10.3 Space Environments

5.10.3.1 The effects (both singular and synergistic) of space environment interactions, e.g., radiation embrittlement, thermal cycling, atomic oxygen (AO), UV radiation, plasma charging, arcing, will be evaluated during hardware design.

Rationale: When exposed to the space environment, material properties can be affected and lead to a greater subsequent susceptibility to additional space environmental effects, e.g. radiation embrittlement leads to greater impact susceptibility, and thermal cycling damage or impact damage to a protective coating on a material leaves the newly exposed material susceptible to AO erosion. Additionally, simultaneous exposure to multiple environmental factors can change the effect from that of each factor individually. The following examples demonstrate this principle:

a. Exposure to UV radiation increases the AO erosion rate of fluorinated polymers such as Teflon® and Tefzel®, sometimes up to an order of magnitude.

b. The Hubble Space Telescope's (HST's) original Wide Field Planetary Camera had a synergistic effect of outgassing contamination, combined with UV radiation, leaving a photo-polymerized contamination deposit that resulted in 50 percent loss in reflectance at the instrument's wavelength of interest. This degradation, along with the spherical aberration, was addressed by instrument replacement on the first HST servicing mission.

5.10.3.2 EEE systems will be designed to meet their reliability requirements when exposed to the ionizing radiation environment defined for the program.

Rationale: Single-event upsets can occur when sitting on the pad and get worse at higher altitudes. Ionizing radiation (IR) dose in orbit can be a hardware lifetime issue. It is critical to involve the IR specialists with the designers as early as possible in the development cycle. Modern low-voltage, high-speed electronics tend to be more IR sensitive than heritage hardware. Design mitigation is typically costly and a schedule threat. Complexities of IR mitigation are underestimated all too frequently in project planning.

5.10.3.3 The vehicle system will be designed to mitigate the effects of spacecraft charging in the space environment defined for the program.

Rationale: Spacecraft charging and electrostatic discharge (ESD) arcs are well-known sources of spacecraft anomalies and failures.

Mitigating the threat of spacecraft charging is accomplished by following well-established spacecraft design techniques to avoid arcing from one point to another on spacecraft surfaces or within the spacecraft systems. Arcing damage resulting from surface charging can be minimized by use of conductive materials on spacecraft surfaces and following standard EMC grounding techniques to assure all external surfaces of a spacecraft will be at the same potential. If partially conductive or insulating materials have to be used on a spacecraft surface, then the differential potentials that may be experienced in the flight environment should be evaluated using a standard surface charging code, or the configuration can be tested in simulated flight environments to demonstrate that any ESD resulting from arcing cannot damage the spacecraft systems. Internal charging is mitigated by implementing adequate shielding to reduce the charging flux to levels where electric fields generated by accumulated charge are insufficient to result in ESD. If this is not possible, then grounding conductors or use of static dissipative materials can reduce the charging threat within the spacecraft. Internal charging threats can be evaluated with internal charging models or with laboratory testing of hardware in flight-like environments.

5.11 Nondestructive Evaluation

NDE is to be performed for fracture-critical hardware and may need to be performed for non-fracture-critical parts**.**

5.12 Operations

This section provides principles by which operational considerations are incorporated into the Design, Development, Test, and Evaluation (DDT&E) phases of the system. These principles aid the program/project management and engineering organizations to achieve life-cycle cost, operational flexibility, and operability targets. Adherence to these design principles influences incorporation of operational efficiencies into the system design and the manufacturing, logistics, maintenance, testing, assembly, integration, prelaunch, postflight, and flight processes.

The operational characteristics of future space systems (supportable, maintainable, reliable, operable, and affordable) affect mission success and program viability, especially affordability. The purpose of this section is to make the performance-driven design community aware of the operational implications of top-level design choices on operational Figures of Merit (FOM), e.g., safety; affordability; environmental compatibility; operational flexibility; life-cycle cost; system availability, system readiness, and mission effectiveness. The intended audience for these *design principles includes operations analysts, space system designers, chief engineers, and program/project/system managers. At each design stage, top-level operational characteristics are considered along with technical performance, safety, and life-cycle cost to achieve a design that appropriately balances these important features. These design principles, applied throughout the DDT&E phases of development through a vigorous and continuous process ensure operational characteristics are properly considered.*

5.12.1 Operations Footprint

5.12.1.1 System designs will be evaluated to ensure that operational characteristics are understood and their effect (people, time, infrastructure, operational flexibility, and cost) on sustaining engineering, ground operations, and flight operations are balanced against the technical performance measures.

Rationale: To achieve and maintain a small operations footprint for the system, operational characteristics and measures should be explicitly known or forecast beginning in the conceptual phase to determine if operationally driven design changes are warranted.

5.12.1.2 Factory-based production, acceptance, and launch site assembly, integration, and checkout tests will be identified from integrated design data when these data become available and the resource effect (people, time, infrastructure development phasing, and cost) on ground operations balanced against the system's technical performance and process definition.

Rationale: The need for fewer tests of this nature restricts the operations footprint of the system, while appropriately providing the critical mission, vehicle, and system integrity. Development, Qualification, and Acceptance Test Plans (drafts) provided at PDR provide early insight into the potential need for factory and launch site test operations, but the actual system design details drive the final answer. Understanding the emerging need for these kinds of tests as early as possible allows timely technical, schedule, and financial response to potentially costly unforeseen activities. (Reference: Applicable specifications within NASA/SP-2007-6105, NASA Systems Engineering Handbook.)

5.12.1.3 With participation from launch site design representation, a resource-loaded functional analysis will be performed for the system, accounting for the known use cases. When possible, one should view the launch vehicle and the launch complex as a single launch system and evaluate each design feature in terms of the integrated effect on performance, schedule, and resources. Ideally, this is performed before the PDR(s) and repeated before the CDR(s) to allow time to influence ongoing design decisions.

Rationale: The launch complex is another stage of the vehicle, defined as stage 0, and has the same importance as any of the other launch vehicle stages or elements. It should not be thought of as a secondary entity that can be addressed later in the design flow. This analysis ensures that all operational constraints and limitations are identified for both the launch vehicle and the launch complex to achieve a single system.

5.12.1.4 Prelaunch processing and pad supportability factors will be considered for all space systems to balance ground and flight system features that result in minimalized necessary and sufficient infrastructure.

Rationale: The less infrastructure the better, provided that all critical functions can be performed and costs are reasonable. A clean pad concept of minimizing infrastructure reduces the risk of debris damage at lift-off, potentially lowers launch complex development and sustaining costs, and facilitates the launch pad's survival and restoration should a serious accident at lift-off occur. Mission and maintenance requirements may drive adding towers and supporting structure to the launch pad, but this should be done only after evaluating potentially viable alternate options, e.g., trade increased part/system reliability cost versus that of service structure, manpower, and equipment required for maintenance.

5.12.1.5 Initial system constraints, limitations, and operating instructions related to maintenance, assembly, integration, checkout, test, and flight need to be provided as early as practical but no later than PDR.

Rationale: This information often drives the need for support equipment, materials, facility capabilities, and training that can affect cost, schedule, and life-cycle (including disposal) products. Early awareness of these needs allows time to evaluate alternative approaches and develop plans for implementation.

5.12.1.6 Transition planning from development to operations (including hardware delivery, facility uses, support equipment, and checkout and testing) will be performed in the CDR timeframe to ensure readiness and operations viability.

Rationale: Effective resource planning and an inventory of everything needed to carry out operations should mitigate risk associated with the handoff of the launch vehicle and supporting assets from development to operations organizations and enable meeting schedule, cost, and resource targets.

5.12.1.7 The full scope of GSE, the hardware that connects to the launch vehicle, should be considered.

a. Resources for its development, procurement, handling, and use should be addressed in parallel with the launch vehicle design.

b. The need for spare GSE should be addressed to ensure its availability at critical times in the schedule.

Rationale: GSE development is often a significant technical undertaking on the overall project's critical path and can require a large expenditure of funds. Recognition of GSE development as a critical parallel project is important to ensure that its availability supports primary mission milestones in a timely manner.

5.12.2 Mission Success

5.12.2.1 For launch vehicles, the DRMs will be used to establish system readiness and launch availability technical measures with a specified confidence level. Ideally, this should happen no later than SDR but can be addressed later, if necessary. In the absence of approved DRMs, the best mission case/use case information derived from the Operations Concept document can be used with the risk of non-viability for some highly desirable missions that were potentials had they been addressed early.

Rationale: The launch vehicle has to perform its role within understood and potentially constrained bands of time to achieve desired mission objectives, e.g., specified orbits, target rendezvous, celestial mechanics driven observations, etc. System readiness and launch availability/launch probability provide an operational metric against which to evaluate the system design to forecast utility and success.

5.12.2.2 Reliability data will be collected and integrated by the Safety and Mission Assurance organization and provided for the PDR milestone, based on known subsystem components when feasible or by comparison with similar systems.

Rationale: It is essential to integrate reliability data early into the iterative supportability and system availability and readiness analysis process to allow success for flight and ground design influence for minimizing operational costs. A lesson learned is that reliability data were still not available months after PDR and were never provided before Constellation shutdown.

5.12.2.3 An assessment of the system design will be performed before vehicle element PDRs to recommend and influence the number and size of access hatches for assembly, integration, and maintenance tasks.

Rationale: The number of hatches into the vehicle maintenance areas needs to be well planned so as not to be the limiting factor in turnaround time and in risk of damage to flight systems.

Inclusion of human factors engineering assures access and operability for ground processing ("every time" access) and LRU/ORU replacement.

5.12.2.4 The mass allocation for flight hardware will include the mass provision for GSE attachment for any space system requiring internal access for ground processing or maintenance.

Rationale: GSE is either attached to flight hardware or supported external to the vehicle. The former method is more common and simpler, and the mass available for an attach point is a limiting factor in the design concept for GSE.

5.12.2.5 Draft releases of subsystem design description documents are recommended to occur at least 3 months before PDR and CDR with updates posted as part of these formal reviews and/or as defined by the project-specific schedule with baseline of these documents 6 months after CDR.

Rationale: Subsystem design definition and evolution are captured to understand how the design has evolved, to document the options that were developed to meet the requirements, and to define why a specific option was chosen. This documentation is the basis for developing operational documentation to describe how each of the subsystems function and serves as a formal document to reflect the current subsystem design baseline that can be used by other teams (software, Instrumentation Program and Command List, Safety & Mission Assurance, other subsystems) to develop their products. These documents represent the subsystem-specific design baselines for a point in time that is consistent across the subsystems. This documentation can be used as an operational and interface analysis tool across the subsystems and as an aid to subsystems in preparation for the formal reviews.

5.12.2.6 An evaluation of telemetry data and identification of ground commands essential for the monitoring and control of the vehicle or system will be performed to appropriately influence the design of the flight and ground system to accommodate operator needs.

Rationale: A process for defining the content of vehicle telemetry for each operational phase/mode should be established and include the operations community in the selection of parameters required for real-time monitoring and post-test/postflight analysis.

5.12.2.7 Design guidelines for instrumentation will be developed to assist avionics, software, and ground systems designers in determining flight system versus ground system function allocation.

Rationale: Guidelines for vehicle versus ground-based instrumentation, established early in the project, are used to determine what instrumentation needs to be incorporated into avionics versus being measured directly by ground systems.

5.12.2.8 To facilitate efficient fault detection and isolation, trades will be conducted to determine the feasibility of reporting anomalies at the LRU level.

Rationale: Self-diagnosing subsystems/components result in efficiency gains in operations, maintenance, and cost savings for ground operations with respect to troubleshooting to isolate a problem down to the LRU level.

5.12.2.9 The time during the launch sequence at which power is switched to internal (vehicle supplied) will allow adequate time for system health verification before ignition.

Rationale: Transitioning to internal power at least 2 minutes before launch allows sufficient time to monitor transition from ground to internal power and to ensure successful transition before resuming countdown. Early Ares I designs called for transition very close to (less than 60 seconds before) launch, causing concern from the operations engineers that insufficient time was being given to assess vehicle electrical power health before launch.

5.12.3 Cost

5.12.3.1 Evaluation of the system to determine candidate LRUs will be performed as early as practical and ideally no later than the vehicle PDR milestone.

Rationale: Approximately 70 percent of life-cycle cost is set by the PDR milestone, which allows a brief window of opportunity to influence hardware design to minimize operational support costs. A robust system design includes LRUs to allow for timely removal and replacement to assist in meeting hardware availability to meet launch schedules and provide for cost-effective maintenance processes.

5.12.3.2 Comparative Cost Analysis that estimates recurring and non-recurring costs will be provided for significant flight and ground hardware design change impacts that affect the system support solution.

Rationale: Cumulative changes over time can add up to significant cost increases without awareness. Comparison costs estimates are used for supporting trade studies, GSE cost projections, sensitivity analysis, etc., and keep costs visually up front for the management team to keep a handle on affordability.

5.13 Propulsion Systems

All flight propulsion systems developed at MSFC will be designed and tested in consideration of best practices and lessons learned, as documented in ER01 Memorandum, MSFC Propulsion Systems Designers' Handbook (MPSDH).* The MPSDH provides historical design practices with supporting historical rationale. These practices will be critically evaluated and adapted for the wide range of missions and risk tolerance scenarios that characterize the missions that MSFC supports.

*NOTE: Copies available from ER/MSFC Propulsion Systems Department.

5.13.1 Liquid Propulsion Systems

5.13.1.1 Main Propulsion Systems (MPSs) for Pump-Fed Engines

In designing an MPS for pump-fed engines, the following functions will be taken into consideration: propellant tank filling and draining; propellant tank pressurization, venting, and relief; propellant delivery to the engine for thermal conditioning and engine operation; pneumatic and/or hydraulic systems for valve control on the MPS, engine, and other stage systems; and purging and inerting of the MPS and engine.

Rationale: MPS may also include propellant storage, auxiliary power, compartment conditioning, hazardous gas detection, umbilical disconnects, instrumentation, and pogo suppression capability. There are a number of considerations that should be addressed in designing the system. Some are levied at the vehicle level, including propellant selection, engine type, and number of engines. Some are derived during the MPS design process such as pressurization method and ullage pressure.

5.13.1.1.1 MPS Integration Requirements

All of the tasks noted in this section will require approval by the Propulsion System Department (PSD) technical authority to assure successful integration.

Rationale: Experience has shown that the complexity of MPS integration requires special expertise to ensure success.

5.13.1.1.2 MPS Test Facility and Launch Facility Integration

5.13.1.1.2.1 The following analyses, operational expertise, and functional expertise will be integrated into the end-to-end launch and test facility requirements design and analyses**:**

a. Tank loading.
b. Tank pressurization and venting.
c. Tank drain.
d. Engine thermal conditioning.
e. Tank, MPS, and engine integrated operation.
f. Inerts supply performance and tank sizing.
g. Pneumatics and/or hydraulics.

5.13.1.1.2.2 The operational performance timeline will include launch facility and test facility vehicle to facility hand-off events.

5.13.1.1.3 MPS Integrated Control Systems

All of the tasks noted in this section will require approval by the PSD technical authority to assure successful integration.

5.13.1.1.3.1 Operational and functional expertise, requirements, and analysis will be included in the development and design of the MPS control algorithms and software that will be integrated into the vehicle control system.

5.13.1.1.3.2 Operational and functional expertise, requirements, and analysis will be included the development and design of real-time control simulations and models that will be integrated into the vehicle control system.

5.13.1.1.4 MPS Integrated Avionics and Instrumentation

5.13.1.1.4.1 Operational and functional expertise, requirements, and analysis will be included for the development and design of MPS avionics and instrumentation to validate MPS system requirements that will be integrated into the vehicle system.

5.13.1.1.4.2 The task will require approval by the PSD technical authority to assure successful integration.

5.13.1.1.5 MPS/Power Integration

5.13.1.1.5.1 Operational and functional expertise, requirements, and analysis will be included for the development and design of power requirements that will be integrated into the vehicle system.

5.13.1.1.5.2 This task will require approval by PSD technical authority to assure successful integration.

5.13.1.1.6 MPS/Vehicle Analytical Integration

All of the tasks noted in this section will require approval by the PSD technical authority to assure successful integration.

5.13.1.1.6.1 The following analyses, operational expertise, and functional expertise will be integrated into the end-to-end vehicle requirements design and analyses:

a. Propellant inventory.
b. Tank loading.
c. Tank pressurization and venting.
d. Tank drain.
e. Engine thermal conditioning.
f. Tank, MPS, and engine integrated operation.
g. Inert supply performance and tank sizing.
h. Pneumatics and/or hydraulics.
i. MPS mass estimates.
j. Boil-off analyses.
k. Slosh analysis.

5.13.1.1.6.2 In preparation for SRR and PDR, MPS system-level trades and risk assessments for integrated system-level testing will be used.

Rationale: Budget phasing and lead times require early definition and planning of MPS testing. Failure to define this major element test to a sufficiently informed level at SRR and to provide full definition before PDR has posed significant programmatic risks in previous programs.

5.13.1.1.7 System-Level Testing

Programs or projects that include development of a new or significantly modified vehicle MPS will include an MPS-level test program or an integrated stage test.

Rationale: The MPS is a highly distributed, thermodynamically and operationally complex integrated system. Analysis and component-level testing alone are insufficient to ensure an integrated system by which the MPS delivers propellants to the engine interface within the property and flow limits that assure safe engine operation. Failure to perform integrated MPS testing imposes risk of engine failure leading to loss of mission and loss of crew (if applicable). Trades can be made whether to use flight-like tanks or facility tanks, whether to test a flight stage or test a propulsion module, and when the testing occurs. These decisions will be based on risk. The testing, at a minimum, should include the pressurization, engine feed, and recirculation systems. Demonstration is not sufficient to cover the range of test conditions that need to be addressed.

5.13.1.2 Pump-Fed Liquid Engines

To adequately design a pump-fed liquid engine properly for a launch vehicle, the following design and development parameters need to be taken into consideration: engine cycle and propellant selected based on performance (Isp), thrust, run duration, propellant mixture ratio, engine weight, envelope size (length and diameter), reliability, pogo suppression capability, TRL of the cycle, testing, components, materials, manufacturing, cost, and schedule. After the design phase, the engine undergoes development testing, followed by qualification and flight acceptance testing, and operation that meets mission and manned rating requirements. The design starts with system requirements and involves extensive analysis, testing, and evaluation to characterize and qualify engine operation during the development process. Engines may be of various types (expander, gas generator, staged combustion, etc.) depending on the vehicle/mission requirements, resulting in a direct impact on how they are designed, manufactured, tested, and operated in flight.

5.13.1.2.1 Integrated System-Level Testing and Analysis

Programs or projects that include development of a new or significantly modified upper stage or in-space liquid rocket engine will include an integrated level stage test program or an integrated stage test.

Rationale: Upper stage or in-space rocket engines require testing in a vacuum, and thermal conditions in space necessitate an integrated system test to mitigate the risk of thermally induced malfunction in the space environments. Engine sea-level and/or vacuum testing alone is insufficient to ensure the integrated system operates properly. Trades can be made whether to use flight-like tanks or facility tanks, whether to test a flight stage or test a propulsion module, and when the testing occurs. These decisions will be based on risk. The testing at a minimum should include the pressurization, engine feed, start ignition, start transient, steady-state operation, and shut-down modes.

5.13.1.3 Propulsion Systems with Pressure-Fed Engines

Propulsion systems with pressure-fed engines find use over the widest range of mission requirements and draw upon the widest range of propellants. They often serve as ascent/launch vehicle auxiliary propulsion systems, reaction control systems for stages and spacecraft, orbital maneuvering systems, robotic lander descent systems, robotic ascent vehicle propulsion systems, and satellite station-keeping systems. Mission durations have historically ranged from minutes to decades. Depending on mission requirements, these systems may be based on any of a wide range of propellants, such as conventional storable monopropellants and bipropellants, advanced non-toxic propellants, cryogenic propellants, inert gases, and reactive gas mixtures. In designing a pressure-fed propulsion system, the following methodologies should be taken into consideration: pressurant loading, storage, and distribution; propellant storage, acquisition, isolation, and delivery; and quantity of thrusters for required impulse and moment generation capability. There are a number of system considerations that should be addressed in designing the system, including propellant selection, pressurization method, desired thrust, pulse-mode operation versus steady-state operations, pulse mode duty cycle capabilities, very large numbers of engine thermal cycles, propellant peculiarities, and propellant management alternatives (surface tension devices, positive expulsion devices, propellant settling, or other more advanced propellant management approaches). Pressurization methods include blow-down mode, blow-down with repressurization, or regulated mode.

5.13.1.3.1 Development Testing

5.13.1.3.1.1 A development cold-flow test article that accurately simulates the internal acoustics of the flight system will be tested to validate that the pressurization and propellant system performance meets the engine inlet conditions under steady-state and transient modes of operation.

Rationale: This test serves to validate that the integrated pressurization and propellant system performance meets the engine inlet conditions under steady-state and transient modes of operation. Failure of this system to perform as intended can lead to loss of the vehicle. This cold-flow test article would be used to correlate fluid models. The cold-flow test article should simulate the internal fluid line geometry, including the placement of turns, valves, orifices, venturis, intrusive flow meters, etc., and should include valves that have the same internal geometry and shuttle times as the flight valves.

5.13.1.3.1.2 Functional testing will be conducted once a reaction control system (RCS) system is assembled and installed on the vehicle in accordance with applicable range safety requirements.

Rationale: Functional testing, including leakage testing, is needed to verify component performance after assembly and installation of the components into the system. Historically, this testing has been performed at the system level to assure no damage or blockage has occurred during assembly. Past programs have tried to take a waiver for this requirement and have resisted using SMC-S-016, Test Requirements for Launch, Upper-Stage and Space Vehicles, specifically paragraph 9.4.2, Propulsion Subsystem Leakage and Functional Tests..

5.13.1.3.1.3 The certification program for RCSs that provide time-critical or performance-critical functions for human-rated vehicles or other high-value missions will include a system-level hot fire test at the appropriate altitude conditions.

Rationale: Hot-fire testing at altitude conditions show the absence of low-frequency combustion instabilities and other chamber/feedline acoustic coupling phenomena that could unexpectedly decrease system performance.

5.13.1.3.1.4 RCSs using propellants with freezing points above -40 °C (-40 °F) for in-space applications with mission times longer than 24 hours will be subjected to a thermal vacuum test at the integrated level, i.e., at a level where the RCS is integrated into a higher level assembly, such as a pod, module, upper stage, or spacecraft. The thermal vacuum test may be conducted without propellants loaded.

Rationale: Thermal vacuum testing needs to be conducted to assure propellant lines do not freeze or undergo freeze-thaw-burst cycles. Testing also assures that resultant propellant conditions at the integrated level remain within the thruster-qualified operational limitations. The -40 °C (-40 °F) is based on lessons learned.

5.13.1.3.1.5 RCSs using propellants with elevated temperature sensitivities will be subjected to a thermal vacuum test at the integrated level, i.e., at a level where the RCS is integrated into a higher level assembly, such as a pod, module, upper stage, or spacecraft. The thermal vacuum test may be conducted without propellants loaded.

Rationale: Thermal vacuum testing needs to be conducted to assure that resultant propellant conditions at the integrated level remain within the thruster-qualified operational limitations.

5.13.1.3.1.6 RCS thruster certification will include thruster-level hot-fire test data at each expected combination of duty cycles and pulse trains and for expected operating condition ranges to accumulate 2.0 (or 1.5) times mission life requirements.

Rationale: This testing is needed to assure the thruster and thruster valve assembly are robust against thermal runaway (hot injector), combustion instability, combustion efficiency (Isp), thruster life (catalyst breakup or chamber coating breakdown), fuel film cooling breakdown (hot chamber conditions), or other related failures in each operating scenario. To understand the system operation, it is good practice to test as the system is planned to operate. Data from this test program provide actual propulsion performance characteristics to inform guidance, navigation, and control (GN&C) models and integrated flight system design.

5.13.2 Solid Propulsion Systems

5.13.2.1 Solid Propulsion Systems Design

Solid propulsion motors will be tested to assure the design is free of combustion instability that may pose vehicle safety or require significant vehicle design effort to mitigate.

Rationale: Combustion instability could result in a structural disintegration of the solid motor and the vehicle or pose significant vibration into the vehicle, such as in the case of thrust oscillations (TOs), requiring an extensive mitigation effort by the vehicle designer, adding weight, complexity and risk to the program.

5.13.2.2 Loads, clearances, and induced environments on the system will be quantified and verified.

Rationale: The motor should be able to integrate with the vehicle and support structures both physically and from an induced-loads perspective. On the Comet Nucleus Tour (CONTOUR) failure, a solid rocket motor (SRM) was submerged too far into the spacecraft; the effects of plume heating were not recognized. TO is another induced-load that has to be considered.

5.13.2.3 Solid rocket plume impingement analysis predictions will be documented as induced environments for the appropriate vehicle elements.

Rationale: On August 15, 2002, the CONTOUR, a part of the NASA Discovery series of solar system exploration satellites, was lost when an integral STAR™ 30BP SRM was fired to leave orbit and begin the transit to the comet Encke. The Mishap Report lists the probable proximate cause as overheating of the CONTOUR spacecraft by the SRM exhaust plume. Significant observations included limited understanding of SRM plume heating environments in space

5.13.2.4 For a new SRM design, full-scale development static test firings will be performed at the minimum and maximum propellant mean bulk temperatures (PMBTs).

Rationale: Performance data are needed over the range of expected PMBTs to allow a valid prediction of performance. This also verifies the joint performance over the temperature range.

5.13.2.5 The qualification test program will static test the motors at extremes of high and low PMBT specified in the requirements.

Rationale: To have valid performance verification, the entire range of PMBT has to be addressed. Extremes of PMBT can also affect components of the solid propulsion system, such as joints. The Challenger (STS-51L) SRM failure is such an example.

5.13.3 Thrust Vector Control (TVC) Systems

5.13.3.1 TVC subsystems will comply with all vehicle performance requirements at worst-case 3-sigma combinations of parameters.

5.13.3.2 TVC subsystem performance requirements are derived from vehicle-level requirements, and compliance will be met under all conditions.

Rationale: To show compliance, dispersion analyses using worst-on-worst conditions ensure the greatest amount of margin between subsystem capability and vehicle needs. However, at a minimum, 3-sigma statistical combinations of parameters in dispersion analyses are sufficient to show performance requirement compliance. In addition, system-level tests should be performed to validate/verify component/system performance and capability.

5.14 Safety, Reliability, and Maintainability

5.14.1 Safety

5.14.1.1 Spacecraft habitable environment venting systems will not vent through outlets that are used to vent other liquids or gases.

Rationale: This prevents gases or liquids from being pulled back into the habitable environment if there is any backflow through the valve. There have been cases where toxic experiment fluids have been released into a habitable volume through a vent valve.

5.14.1.2 An inhibit switch will be provided in each sensor circuit to allow isolation of a single malfunctioning sensor and permit normal operation of all other remaining sensing units.

Rationale: This allows continued monitoring after one sensor failure. A physical switch may not be required if the function can be provided by software systems.

5.14.1.3 For crewed space systems, electrical shock protection circuits will be totally redundant to ensure crew protection in the event of primary shock protection circuit failure.

Rationale: This provides two fault tolerances for a catastrophic event

5.14.2 Reliability

5.14.2.1 Design should use proven technologies.

Rationale: Proven technology is essential for good design and reliability. Flight designs should be TRL greater than 7, and when using designs below TRL 7, the risk to reliability needs to be understood.

5.14.2.2 Design should use proven design methods.

Rationale: Proven design is essential for good design and reliability. Proper qualification and certification of designs should be addressed based on previously flown designs.

5.14.2.3 Design should use proven processes, i.e., manufacturing, assembly.

Rationale: Well-understood processes are essential to prevent defects, etc., are at the center of design reliability, and are essential for improved process reliability.

5.14.2.4 Design should use good quality control practices.

Rationale: Good quality control practices result in high process reliability and robust design and prevent defects, faults, etc. Lack of good quality control practices can result in situations like those encountered with Shuttle foam issues, specifically those on Columbia.

5.14.2.5 A system should operate within the design environment/specification.

Rationale: Proven operation in the design environment/specification is essential for good design and reliability. Lack of highly reliable designs in the design environment can result in situations like the O-ring problem during Challenger and the thermostatic switch during Apollo 13, which was designed for 28 Vdc and operated at 65 Vdc,

5.14.2.6 Use of proven components of known reliability should be used to the highest extent possible.

5.14.2.7 Component selection should be based on the worst-case environment usage.

5.14.2.8 Ability to check the condition of critical components should be provided.

5.14.2.9 Warning or indication of loss of failure detection should be provided for critical components or systems.

5.14.2.10 Where redundant hardware or software is used to satisfy reliability requirements, the system should monitor the health of all redundant elements.

5.14.2.11 Systems, components, and elements should be isolated from each other so that failure of one does not cause failure of another.

5.14.2.12 Critical systems should be designed with redundant or backup systems to enable continued function after any critical failure.

5.14.2.13 Where redundant hardware or software is used to satisfy reliability requirements, the system should automatically switch over from a failed element to the redundant element.

5.14.2.14 Systems design should consider the failure modes, so that systems are designed to be failure tolerant to catastrophic events.

Rationale: Failure paths should be designed to control and direct the effects of failure in a way that limits its safety impact.

5.14.2.15 Systems should be designed with the ability to sustain damage from their failure effects and limit the safety impact to personnel and crew.

5.14.2.16 Critical systems elements should be designed so that failure of the primary and redundant systems cannot be caused by a single credible event, e.g., contamination, explosion, temperature, vibration, shock, acceleration, and acoustics.

Note: Other design practices can be found in NASA Technical Memorandum 4322, NASA Reliability Preferred Practices for Design and Test, http://klabs.org/DEI/References/design_guidelines/nasa_reliability_preferred_practices.htm. Retrieved 08-28-14.

5.14.3 Maintainability

5.14.3.1 Design should allow use of common tools and maintenance hardware.

5.14.3.2 Design should enable ORU changeout and planned equipment reconfiguration by personnel wearing clothing appropriate to the environment and phase of flight.

5.14.3.3 The design should preclude the use of destructible circuit protection devices, such as fuses during dynamic flight phases.

5.14.3.4 Design has to consider standardization.

5.14.3.5 Equipment design for on-orbit maintenance will consider intravehicular activity as the prime resource.

5.14.3.6 Facilities, equipment, and software design will allow reconfiguration and growth during the mission life.

5.14.3.7 Systems and subsystems will be as functionally, mechanically, electrically, and electronically independent as practical to facilitate maintenance.

5.14.3.8 Equipment design will reduce to a minimum the incidence of preventive and corrective maintenance.

5.14.3.9 Equipment design will minimize maintenance complexity.

5.14.3.10 Equipment design will minimize the time requirements for maintenance and checkout and test.

5.14.3.11 Maintenance equipment and tools will be kept to a minimum (design for commonality).

5.14.3.12 Critical systems will be capable of undergoing maintenance without the interruption of critical services.

5.14.3.13 Notification of loss of operational redundancy will be provided immediately to the crew.

5.14.3.14 Quick-disconnect connectors will be used for items requiring maintenance actions where allowable.

5.14.3.15 Soldering, welding, brazing, and similar operations during maintenance will be minimized.

5.14.3.16 Sufficient space will be provided for maintenance actions and preclude the introduction of hazardous conditions during maintenance procedures or diagnostics.

5.14.3.17 Items most critical to system operation and that require rapid maintenance will be most accessible.

5.14.3.18 When relative criticality is not a factor, items requiring most frequent maintenance actions will be most accessible.

5.14.3.19 Each equipment access will be labeled to indicate items that are visible or accessible through it.

5.14.3.20 Systems will be designed to facilitate removal and replacement of components and subsystems without damage to or disturbing other components or subsystems.

5.15 Software

5.15.1 In the software design, mechanisms will be provided to detect credible system faults and to react to these faults according to a pre-described plan.

Rationale: Without the capability to safely recover from certain credible faults, the system could lose data, harm an instrument, or, in the worst case, cause loss of life or end of the mission.

5.15.2 A safety-critical and security-critical coding standard will be implemented on all mission-critical software and verified by static analysis tools.

Rationale: An essential element of safety and security coding in the C programming language is a set of well-documented and enforceable coding rules. All rules are meant to be enforceable by static analysis. The coding standard specification should enumerate both safe and secure coding rules and require analysis engines to diagnose violations of these rules as a matter of conformance to the specification. Consistent use of approved coding standards reduces the frequency of common run-time errors, unsafe coding practices, and unsecure coding practices and promotes maintainability and re-usability.

5.15.3 Software will be designed to verify the integrity of all inputs and outputs in the control system.

Rationale: Systems have to use accurate data to maintain state information and produce correct output messages.

5.15.4 A policy for eliminating unreachable code or mitigating the risk of any unreachable code will be established.

Rationale: Code that is believed to be unreachable poses a residual risk to the system in the event that it is executed inadvertently.

5.15.5 Software will be designed to protect against incorrect use of memory.

Rationale: Incorrect use of memory can lead to catastrophic failure.

5.15.6 Flight software will be designed to initialize software and hardware to a known, safe, and deliberate state.

Rationale: Upon startup, flight systems need to autonomously enter a state that requires no immediate ground intervention to ensure its health and safety and that preserves vital system resources, even in the presence of faults.

5.15.7 Software will be designed to handle invalid data appropriately.

Rationale: The ability to continue operating in the presence of invalid data and react appropriately can prevent responses that lead to hazardous conditions.

5.15.8 Quantitative margins for all critical resources will be established and maintained, allowing for maturation of usage estimates through the life cycle.

Rationale: Computing resources tend to become problematic late in the development process. Design margins help identify problems earlier and provide a means of managing them.

5.15.9 A robust and well-thought-out response to resource oversubscription situations will be included in the software design.

Rationale: Resource oversubscription is a severe fault condition that can lead to unpredictable behavior of the software system and render it inoperable. Timely detection and planned response to oversubscriptions can preserve critical system capabilities.

5.15.10 Timely visibility into the use of computing resources will be incorporated into the software design.

Rationale: Measurement of resource usage enables determination and validation of operating margins throughout the life cycle of the project; these can be indicators of potential error and fault conditions. It also enables measurement of critical computing resources, thereby maximizing the prospects for safe and reliable operation of the software.

5.15.11 Required pre-conditions and post-conditions at software transitions will be asserted.

Rationale: Assuming that pre-conditions and post-conditions are met can lead to hazardous situations and system malfunction.

5.15.12 The software design will include the capability for commanding modification of the software and for preventing unwanted modifications.

Rational: There is often a need for modification of the software or data components after delivery to correct faults, improve performance, maintain hardware functionality or other attributes, or adapt to a changed environment. The capability is needed in flight via the uplink command function and before launch via the umbilical link. Additionally, software that is modifiable during operation should be protected from unintended modifications, including those caused by single-event effects and hardware problems.

5.15.13 Interaction between threads will be designed to prevent inappropriate interference.

Rationale: Multi-threaded software typical of mission-critical embedded applications is vulnerable to incorrect or unpredictable behavior if the interaction between threads has not been adequately designed to prevent inappropriate interference.

5.15.14 Both internal and external commanding will be designed to place the system into an explicitly specified state.

Rationale: Making assumptions about the system state can lead to malfunctions.

5.15.15 Safety-critical software, including data, will be protected from inadvertent modification by non-safety-critical software via partitioning, semaphores, or other means.

Rationale: This protection ensures that software that implements hazard controls works properly.

5.15.16 Software initiating "must-work" functions will possess a means of success detection and have a secondary means of execution when determined to have been unsuccessful.

Rationale: These capabilities ensure that software works properly.

5.16 Structures

5.16.1 Loads for all conditions will be assessed to define bounding cases for use in structural analysis.

5.16.2 Designs using advanced manufacturing methods, e.g., additive, computer numerical control, should provide computer-aided design (CAD) models and assist in a producibility analysis.

Rationale: Producibility analysis software requires three-dimensional (3D) CAD models as input for manufacturing assessment. Two-dimensional (2D) CAD drawings do not satisfy this requirement. These producibility tools depend upon 3D geometry. If only 2D models are provided, resources are wasted to recreate 3D models. If designers provide models to manufacturing, then manufacturing personnel can perform reliable analysis without questioning the pedigree of the models.

For example:

a. A propellant tank gore panel pinning location was incorrectly placed on a fixture. This issue was not found before manufacturing activities because of incomplete models being given to manufacturing for analysis.

b. An unacceptable interference condition occurred between the Robotic Weld Tool and Ares I Common Bulkhead aft y-ring. The interference made the weld impossible to perform. This issue was discovered 2 years in advance, using manufacturing simulation tools. The design of the y-ring was modified, and the weld was successfully completed 2 years later.

c. Manufacturing simulation with appropriate models allowed discovery of kinematic problems with the Verval tool, which was used to perform pull plug welds. Joint limitations on joints 2 and 3 prevented the tool from performing the required pull plugs. Resolution of the issue took approximately 12 to 14 months from the time the problem was found until the machine was modified on the floor. The issue was discovered early enough that no impact to the schedule occurred.

d. An interference condition with high-pressure hoses on the Robotic Weld Tool and the weld fixture was discovered during manufacturing. Hoses were rerouted to avoid contact during welding operations.

In summary, the successes listed above were possible because of reliable and available 3D CAD models. When incorrect models were provided, errors slipped through and made it to the manufacturing floor, causing delays.

5.16.3 Structural Dynamics Loads and Environments

A structural dynamics loads and environments development/control plan should be generated covering the hardware life-cycle phases from design to flight.

Rationale: Traditionally, no single structural loads and dynamics requirements document or standard meets the needs for the design of all space-flight hardware. This plan should define the process flow of the inputs, analysis, uncertainty, conservatism, results, documentation, testing, and verification and validation for development of the structural dynamic loads and environments for the hardware. This plan should be approved by the appropriate MSFC technical authority.

5.16.4 Vibroacoustics and Shock Environments

5.16.4.1 The level of the maximum predicted environment (MPE) will be that not exceeded on at least 97.5 percent of operational missions, estimated with 50-percent confidence level (P97.5/50 level).

5.16.4.2 Qualification testing will be conducted at levels derived at the MPE level with test tolerances specified in sections 6.3 and 7.6 of MSFC-STD-3676, Development of Vibroacoustics and Shock Design and Test Criteria.

5.16.4.3 Acceptance testing will be conducted 6 dB below the corresponding qualification test.

5.16.4.4 Shock response spectrum criteria are defined for use in developing test criteria not used as analyses input.

5.17 Systems Engineering

Content may be added to this section in the future.

5.18 Test

5.18.1 Test planning should include traceability between the test article and the flight hardware with respect to items such as configuration, fidelity, and boundary conditions. A “test as you fly” approach is recommended as much as possible.

Rationale: Fewer differences between the test and the flight configuration provide a more direct flight rationale.

5.18.2 The organization requesting the test will need to provide the necessary requirements to the organization responsible for performing the test.

Note: The requirements mature during the different phases of the program or project but generally include items such as:

a. Description of the test article (dimensions, weight, axes definition, interfaces, etc.)

b. Test-related interface points (fluid, mechanical, facility, fixture, etc.)

c. Test conditions, durations, and limits, along with allowable tolerances,

d. Number and sequence of desired tests.

e. Cleanliness/contamination requirements.

f. Lifting, handling, and storage requirements.

g. Instrumentation type, count, location, and accuracy required.

h. Data acquisition and delivery requirements (channel count, recording rates, data format, measurement uncertainty, etc.)

i. Photo and video requirements.

j. Quality Control requirements and mandatory inspection points.

k. Any/all known hazards or process requirements associated with preparing for and conducting test operations for the given test article(s).

l. Test documentation requirements (data delivery format, test procedures, test reports, etc.)

Test requirements need to be identified and documented as early in the design process as possible to avoid significant facility and resource impacts late in the flow. Decisions made during the verification planning phase should involve the test organization for feasibility of verification-by-test decisions. Cost and schedule are usually very tight, with any reserves *exhausted by the test phase of a program. Coordination with testing organizations/facilitates is critical to effectively and efficiently plan test programs.*

5.19 Thermal

This section addresses the thermal design, analysis, and margin guidance that would apply to MSFC launch vehicles, spacecraft, instruments, and payloads. There is interdependence between the thermal design and various disciplines across engineering.

5.19.1 Establishment of Thermal Design Requirements

The thermal design requirements for a project are often a combination of known temperature limits and derived temperature/energy requirements that are an artifact of performance requirements. The thermal engineer should integrate with all relevant design disciplines to establish the underlying derived requirements, e.g., structural design, avionics, components, scientific instruments, propellant/pressurization/engine systems, materials, payload accommodations.

Rationale: Most projects begin without explicit thermal requirements. It is imperative for the thermal engineer to communicate across the design and discipline teams early in the project to derive the requirements implied by the function or performance of a system, subsystem, or component.

5.19.2 Thermal Design Margins

5.19.2.1 Establishment of Thermal Design Margins

Thermal design margins should be defined on all components/systems/subsystems at the beginning of the preliminary design phase. This includes temperature margins, heat load margins, etc., for avionics, pyrotechnics, other powered flight components, structures, MPSs, engines, science instruments, etc. These margins (if any) may be phased as a function of design maturity, available test data, program risk level, etc., over the course of the project. Some specific suggested margins are discussed in the following sections.

Rationale: Thermal design margins are difficult to define in a generic way that will apply to all types of systems and components; hence, unlike most disciplines, there is no general standard that can be levied. Each project should define a philosophy and do so early in the project since the approach could affect design and test requirements. It is a lesson learned from previous MSFC projects that the margin is not evenly applied, and there can be issues late in the program during requirements compliance verification caused by not having the margin philosophy clearly outlined.

5.19.2.2 Avionics and Powered Component Thermal Analysis Uncertainty Margin

A temperature margin is typically maintained between the maximum and minimum worst-case thermal analysis prediction and the acceptance test temperature for avionics and other powered components. An additional qualification test margin beyond acceptance is also typically applied.

Rationale: There are numerous uncertainties inherent to an analysis prediction that must be encompassed in determining test level even when worst-case assumptions are used. Allowable prediction levels and the test margin philosophy should be established (as stated in section 5.19.2.1) because, depending on the amount of testing and the nature of the uncertainties, as much as 17 °C (63 °F) may be prudent for passive thermal control designs as detailed in MIL-STD-1540C, Product Verification Requirements for Launch, Upper Stage, and Space Vehicles.

5.19.2.3 Liquid Propellant Thermal Control Margin

A margin of at least 10 °C (50 °F) is recommended to avoid liquid propellant, e.g., hydrazine, freezing or over temperature.

Rationale: This is a critical margin for propulsion system performance and mission safety. The 10-°C (50-°F) margin is consistent with JPL DocID 43913, Design, Verification/Validation & Ops Principles for Flight Systems (Design Principles).

5.19.2.4 Active Thermal Control Margin

It is recommended that active thermal control margin, e.g., pumped loop radiator cooling systems, heat pipes, maintain a 25-percent energy margin.

Note: A larger margin during earlier design phases is prudent to ensure that the 25 percent is maintained after all testing and model correlation is completed.

Rationale: The purpose is to ensure that positive thermal control authority exists during the design phase of the flight system thermal control.

5.19.2.5 Cryogenic Thermal Control Margin

Vehicle cryogenic propellant systems or scientific cryogenic dewar systems should establish a heat leak budget/allocation. It is recommended that a heat leak margin of at least 25 percent be maintained when taking into account all heat transfer sources in meeting stratification, boiloff, or other thermodynamic conditions, such as engine propellant inlet requirements.

Note: A larger margin during earlier design phases may be prudent to ensure the 25 percent is maintained after all testing and model correlation is completed.

Rationale: Small heat loads in the range of a few milliwatts to tens of watts can have large adverse thermal impacts on some cryogenic systems. The total load is comprised of the active and parasitic heat loads.

5.19.3 Thermal Control Heaters

5.19.3.1 Actively controlled heaters should have a maximum duty cycle of 80 percent for worst-case cold conditions, e.g., worst-case cold environments, minimum voltage.

Note: A lower duty cycle during earlier design phases is prudent to ensure the 80 percent is not exceeded after all testing and model correlation are completed.

5.19.3.2 The thermal engineer typically sizes the heater power requirement analytically for a given thermostatic control temperature range. Thermal should coordinate with the avionics and power groups to determine the circuit design (with appropriate redundancy, wire gauge, etc.,) thermostat setpoints or control system parameters, current limits, etc. The engineer should assess the power density of the heaters and coordinate with design for the proper installation/attachment techniques to avoid heater failures.

5.20 Vehicle Management

5.20.1 The vehicle design will provide data necessary to confirm execution of mission objectives.

Rationale: Following this principle assures access to critical mission data.

5.20.2 The vehicle design will provide data modes and formats necessary to indicate the system state and ensure proper chronological mission event execution.

Rationale: Following this principle provides special telemetry to enable operations to diagnose spacecraft emergencies, ensuring that test/diagnostic code is designed and incorporated into the software early and is accessible through flight interfaces, so that problem resolution can be done rapidly and easily at element and flight system level in development and during flight operations. Mission-critical event data and visibility of mission-critical errors should be available via real-

time telemetry for diagnostic use on the ground or during testing. A hierarchical approach should be used so that assessment of spacecraft health/safety can be rapidly attained.

5.20.3 The boot implementation of the flight computer(s) software will include a minimalist configuration that provides the required on-board resources for vehicle safety and ground intervention.

Note: This configuration would include the ability to boot without resources that are of higher risk or are not strictly required for safing. For example, some missions have included a separate flight software version capable of minimal operations without the file system.

Rationale: For certain mission-critical events, ground response may not be possible, and the autonomous fault protection design should ensure completion in the event of a single fault.

5.20.4 The vehicle design will provide capability for the flight computer to autonomously manage and perform nominal and off-nominal missions for crewed and non-crewed vehicles.

Rationale: This is necessary to alleviate the need for human-in-the-loop control of the vehicle, as this is not feasible. Also, there is insufficient capability to control the vehicle during flight via ground communications. Performing this function requires rigorous integration with all subsystems that are necessary to fly and control the vehicle in each mission phase/mode to capture proper functionality, ensure proper chronological mission event sequencing, and correctly embed this functionality into algorithms used by the flight computer.

5.20.5 The vehicle design will protect against human input that could result in loss of critical functions that would impact mission objectives or crew safety.

Rationale: Inadvertent operations could result in the loss of crew/mission. It is imperative that the operator know of hazardous operations and inhibits before execution of a hazardous operation, i.e., enable command before a potentially hazardous command.

5.20.6 For a human-rated vehicle, if a system failure can lead to a critical hazard, the system will have two independent, verifiable inhibits (single fault tolerant).

Rationale: Past experience has shown that failure of systems occurs often enough that a single failure of an inhibit leading to a critical hazard is not acceptable.

5.20.7 For a human-rated vehicle, if a system failure can lead to a catastrophic hazard, the system will have three independent, verifiable inhibits (dual fault tolerant).

Rationale: NPR 8705.2, Human Rating Requirements for Space Systems, states that "The space system shall provide failure tolerance to catastrophic events (minimum of one failure tolerant), with the specific level of failure tolerance (one, two or more) and implementation (similar or dissimilar redundancy) derived from an integrated design and safety analysis." Past experience has proven that only the requirement for "one failure tolerant" is seen by designers, while "minimum" and "derived by safety analysis" are ignored.

APPENDIX A
DOCUMENTS COMMONLY USED BY THE MSFC ENGINEERING COMMUNITY OF PRACTICE

Discipline	Number	Standard
General Principles	AIAA S-120-2006	Mass Properties Control for Space Systems
	ESMD-HEC.Reqt-6.2011	ESMD/SOMD Human Exploration Capabilities Requirements
	MGM 7120.3	MSFC Data Management Guidance
	MGM 8040.1	MSFC Configuration Management
	MPR 2190.1	MSFC Export Control Program
	MSFC-STD-2806	MSFC Tailoring Standard for the Global Drawing Requirements Manual (GDRM) Tenth Edition
	NID 1600.55	NASA Interim Directive: Sensitive But Unclassified (SBU) Controlled Information
	NPR 8705.2	Human-Rating Requirements for Space Systems
	NPR 8715.3	NASA General Safety Program Requirements
Models & Simulations	NASA-STD-7009	Standard for Models and Simulations
Pyrotechnic Devices	JSC-62809 Rev D	Human Rated Spacecraft Pyrotechnic Specification
	MSFC-SPEC-3635	Pyrotechnic System Specification
Aero Sciences		Content will be added in the future.
Electrical Power **EEE Parts** **Electrical Integration** **Electrical Systems and Electronics Design** **Electronic Packaging and Manufacturing** **Power and Energy Systems**	AIAA S-111-2005	Qualification and Quality Requirements for Space Solar Cells
	AIAA S-112-2005	Qualification and Quality Requirements for Electrical Components on Space Solar Panels
	AIAA S-122	Electrical Power Systems for Unmanned Spacecraft
	ANSI/ESD S20.20	For the Development of an Electrostatic Discharge Control Program for the Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)
	FAA AC-20-136A	Aircraft Electrical and Electronic System Lightning Protection
	IPC-6011	Generic Performance Specification for Printed Boards
	IPC 6012	Qualification and Performance Specification for Rigid Printed Boards
	IPC 6012, w/ Amendment 1, Class 3/A	6012B Performance Specification Sheet for Space and Military Avionics
	IPC 6013, Class 3	Qualification and Performance Specification for Flexible Printed Boards
	IPC 2221	Generic Standard on Printed Board Design
	IPC 2222	Sectional Design Standard for Rigid Organic Printed Boards
	IPC 2223	Sectional Design Standard for Flexible Printed Boards

	J-STD-001FS	Space Applications Electronic Hardware Addendum to J-STD-001F, Requirements for Soldered Electrical and Electronic Assemblies
	JSC 20793	Crewed Space Vehicle Battery Safety Requirements
	MIL-STD-461	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment
	MIL-STD-464	Electromagnetic Environmental Effects Requirements for Systems
	MSFC-RQMT-2918	Requirements for Electrostatic Discharge Control; for in-house projects only; meets ANSI/ESD S20-20
	MSFC-STD-3012	Electrical, Electronic, and Electromechanical (EEE) Parts Management and Control Requirements for MSFC Space Flight Hardware
	MSFC-STD-3619	MSFC Counterfeit Electrical, Electronic, and Electromechanical Parts Avoidance, Detection, Mitigation, and Disposition Requirements for Space Flight and Critical Ground Support Hardware
	MSFC-STD-3620	MSFC Electrical, Electronic, Electromechanical (EEE) Parts Obsolescence Management and Control Requirements
	NASA-STD-4003A	Electrical Bonding for NASA Launch Vehicles, Spacecraft, Payloads, and Flight Equipment
	NASA-STD-8739.1A w/Change 2	Workmanship Standard for Polymeric Application on Electronic Assemblies
	NASA-STD-8739.4 w/Change 6	Crimping, Interconnecting Cables, Harnesses, and Wiring
	NASA-STD 8739.5	Fiber Optic Terminations, Cable Assemblies, and Installation
	NESC #06 063 I	NASA Guidelines for Selection and Application of DC/DC Converters
	NPD 8730.2C	NASA Part Policy
	NPR 2570.1	NASA Radio Frequency (RF) Spectrum Management Manual
	RTCA DO-160	Environmental Conditions and Test Procedures for Airborne Equipment (sections 22 and 23)
	SAE ARP5412A	Aircraft Lightning Environment and Related Test Waveforms
	SAE ARP5414	Aircraft Lightning Zone
	SAE ARP5416	Aircraft Lightning Test Effects
	SAE ARP5577	Aircraft Lightning Direct Effects Certification
	SAE AS5698	Space Power Standard
Fault Management	ESMD-HEC.Reqt-6.2011	ESMD/SOMD Human Exploration Capabilities Requirements
	NASA-HDBK-1002	Fault Management Handbook
	NASA/SP-2007-6105	NASA Systems Engineering Handbook
	NPR 8705.2	Human-Rating Requirements for Space Systems

	NPR 8705.5	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects
Flight Mechanisms	NASA-STD-5017	Design and Development Requirements for Mechanisms
Guidance, Navigation, and Control	NASA/SP-8015	Guidance and Navigation for Entry Vehicles
	NASA/TM-2008-215106	GN&C Engineering Best Practices For Human-Rated Spacecraft Systems
Human Systems Integration	ASME Y14.100	Engineering Drawing Practices
	ASME Y14.4	Pictorial Drawing
	ASME Y14.5M	Dimensioning and Tolerancing
	ESA PSS-03-70 Issue 1	Human Factors
	FAA-HF-STD-001	FAA Human Factors Design Standard (HFDS)
	MIL-STD-130M	Identification Marking of U.S. Military Property
	MSFC-STD-267A	Human Engineering Design Criteria (first Agency human factors Standard)
	MIL-STD-961	Defense and Program-Unique Specifications Format and Content
	MIL-STD-1472	Human Engineering (current revision is G). Recommend all previous revisions over Rev. G.
	MSFC-HDBK-3644	Design Product Packages for Launch Vehicle Integration Handbook
	MSFC-STD-555	MSFC Engineering Documentation Standard
	MSFC-STD-3676	Development of Vibroacoustic and Shock Design and Test Criteria
	NASA-STD-(I)-0007	NASA Computer-Aided Design Interoperability
	NASA-STD-3001	NASA Space Flight Human-Systems Standard, in particular, Vol. 2, Human Factors, Habitability, and Environmental Health
	NASA-STD-6002	Applying Data Matrix Identification Symbols on Aerospace Parts
Materials, Processes, and Manufacturing	http://maptis.nasa.gov	Materials and Processes Technical Information System (MAPTIS)
	CHM-17	Composite Materials Handbook
	MMPDS	Metallic Material Properties Development and Standardization (MMPDS)
	MSFC-RQMT-3479	Fracture Control Requirements for Composite and Bonded Vehicle and Payload Structures
	NASA STD 5001A	Structural Design and Test Factors of Safety for Spaceflight Hardware
	NASA-STD-5009	Nondestructive Evaluation Requirements for Fracture-Critical Metallic Components
	NASA-STD-5019	Fracture Control Requirements for Spaceflight Hardware

	NASA-STD-6016	Standard Materials and Processes Requirements for Spacecraft Regulatory Considerations for Cadmium Plating
Mechanical Systems	MSFC-STD-486	Standard, Threaded Fasteners, Torque Limits for
Meteoroids and Orbital Debris	NPR 8715.3C	NASA General Safety Program Requirements (w/Change 4 dated 7/20/09)
Natural Environments	MIL-STD-1809	Space Environment for USAF Space Vehicles
	NASA-HDBK-4002A	Mitigating In-Space Charging Effects – A Guideline
	NASA-HDBK-4006	Low Earth Orbit Spacecraft Charging Design Handbook
	NASA-STD-4005	Low Earth Orbit Spacecraft Charging Design Standard
	NASA/TM-2008-215633	Terrestrial Environment (Climatic) Criteria Guidelines for use in Aerospace Vehicle Development, 2008 Revision
	NASA TP 2361	Design Guidelines for Assessing and Controlling Spacecraft Charging Effects
	NPR 8715.3C	NASA General Safety Program Requirements
Non-Destructive Evaluation	MSFC-RQMT-3479	Fracture Control Requirements for Composite and Bonded Vehicle and Payload Structures
	NASA-STD-5009	Nondestructive Evaluation Requirements for Fracture-Critical Metallic Components
Operations	MSFC-HDBK-2221	Verification Handbook Vol 1: Verification Process
	MSFC-HDBK-3074	Selection Methodology for Orbital Replacement Units
	NASA/SP-2007-6105	NASA Systems Engineering Handbook
	NASA-STD-5005C	Standard for the Design and Fabrication of Ground Support Equipment
	NPD 7500.1	Program and Project Life-Cycle Logistics Support Policy
Propulsion Systems	ER01 Memorandum	MSFC Propulsion Systems Designers' Handbook (MPSDH). NOTE: Copies available from ER/MSFC Propulsion Systems Department
	AIAA S-080	Space Systems - Metallic Pressure Vessels, Pressurized Structures and Pressure Components
	AIAA S-081	Space Systems - Composite Overwrapped Pressure Vessels (COPVs)
	Federal Standard 595 codes	Color codes
	MIL-STD-1540	Product Verification Requirements for Launch, Upper Stage, and Space Vehicles
	NASA-STD-5017	Design and Development Requirements for Mechanisms
	SMC-S-016	Test Requirements for Launch, Upper-Stage and Space Vehicles
Safety, Reliability, and Maintainability	NASA-STD-3001	NASA Space Flight Human-System Standard Vol. 2: Human Factors, Habitability, and Environmental Health
	NASA Technical Memorandum 4322	NASA Reliability Preferred Practices for Design and Test
	QD-R-001	Failure Mode and Effects Analysis and Critical Items List

Software	ISBN 03212711505	CMMI for Development Guidelines for Process Integration and Product Improvement
	MGM 7120.3	MSFC Data Management Guidance
	MGM 8040.1	MSFC Configuration Management
	MPR 1410.1	Organizational Issuances
	MPR 7150.1	MSFC Software Engineering Requirements
	NASA-STD-8719.13	NASA Software Safety Standard
	NASA-STD-8739.8	NASA Software Assurance Standard
Structures **Stress and Fracture Analysis** **Dynamics Analysis, Loads, and Model Standards**	CMH-17	Composite Materials Handbook
	ES22 Memorandum	Transportation and Handling Limit Load Factors NOTE Copies available from ES/MSFC Thermal & Mechanical Analysis Branch.
	MMPDS-08	Metallic Material Properties Development and Standardization (MMPDS)
	MSFC-HDBK-505	Structural Strength Program Requirements (Typically used only for heritage hardware for which this document was applicable and generally not used for new design within EV)
	MSFC-RQMT-3479	Fracture Control Requirements for Composite and Bonded Vehicle and Payload Structures
	MSFC-STD-3676	Development of Vibroacoustic and Shock Design and Test Criteria
	NASA-SP-106	The Dynamic Behavior of Liquids in Moving Containers
	NASA-STD-5001	Structural Design and Test Factors of Safety for Spaceflight Hardware
	NASA-STD-5002	Load Analyses of Spacecraft and Payloads
	NASA-STD-5018	Strength Design and Verification Criteria for Glass, Ceramics, and Windows in Human Space Flight Applications
	NASA-STD-5019	Fracture Control Requirements for Spaceflight Hardware
	NASA-STD-5020	Requirements for Threaded Fastening Systems in Spaceflight Hardware
	NASA-STD-8719.9	Standard for Lifting Devices and Equipment
Systems Engineering	MPR 7120.1	MSFC Engineering and Program/Project Management Requirements
	MPR 7123.1	MSFC Systems Engineering Processes and Requirements
	MSFC-HDBK-3173	Project Management and Systems Engineering Handbook
	NASA/SP-2007-6105	NASA Systems Engineering Handbook
Test		Content will be added in the future.
Thermal	JPL DocID 43913	Design, Verification/Validation & Ops Principles for Flight Systems (Design Principles)
	MIL-STD-1540	Product Verification Requirements for Launch, Upper Stage, and Space Vehicles
	NASA-STD-7002	Payload Test Requirements
Vehicle Management	NPR 8705.2	Human-Rating Requirements for Space Systems (w/change 1 dated 12/7/2009)

APPENDIX B
ACRONYMS AND ABBREVIATIONS

&	And
ºC	Degree-Celsius
°F	degree Fahrenheit
%	percent
®	registered trademark
™	trademark
2D	two dimensional
3D	three dimensional
AIAA	The American Institute of Aeronautics and Astronautics
ANSI	American National Standards Institute
AO	atomic oxygen
AR	Acceptance Review
ARP	Aerospace Recommended Practice
ASME	The American Society of Mechanical Engineers
CAD	computer-aided design
cm	centimeter
CDR	Critical Design Review
CMH	Composite Materials Handbook
CMMI	Capability Maturity Model Integration
CONTOUR	Comet Nucleus Tour
COPV	composite overwrapped pressure vessels
CPU	central processing unit
da/dN	crack length extension per cycle
dB	decibel
dB(A)	A-weighted decibel
dc	direct current
DCB	Document Control Board
DCR	Design Certification Review
DDT&E	design, development, test, and evaluation
DRM	Design Reference Mission
EEE	electrical, electronic, and electromechanical
EEPROM	electrically erasable programmable read only memory
EMC	electromagnetic compatibility
EMI	electromagnetic interference
ESA	European Space Agency
ESD	electrostatic discharge
ESMD	Exploration Systems Mission Directorate
ET	External Tank
FAA	Federal Aviation Administration

FMEA	Failure Modes Effects Analysis
FOM	Figures of Merit
GDRM	Global Drawing Requirements Manual
GN&C	guidance, navigation, and control
GSE	ground support equipment
HDBK	Handbook
HEC	Human Exploration Capabilities
HF	human factors
HFDS	Human Factors Design Standard
HST	Hubble Space Telescope
(I)	Interim (Standard)
in	inch
IPC	Association Connecting Electronics Industries
IR	ionizing radiation
ISBN	International Standard Book Number
Isp	specific impulse
ISS	International Space Station
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
K1c	fracture toughness
LRU	line replaceable unit
M&P	materials and processes
MAPTIS	Materials and Processes Technical Information System
MGM	Marshall Guidance Manual
MIL	military
MMPDS	Metallic Materials Properties Development and Standardization
MPDMS	Multiprogram Document Management System
MPE	maximum predicted environment
MPR	Marshall Procedural Requirements
MPS	Main Propulsion System
MPSDH	MSFC Propulsion Systems Designers' Handbook
MRL	Material Readiness Level
MSFC	Marshall Space Flight Center
MUA	material usage agreement
mW	milliwatt
N/A	not applicable
NASA	National Aeronautics and Space Administration
NDE	nondestructive evaluation
NESC	NASA Engineering and Safety Center
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OPR	Office of Primary Responsibility
ORU	orbital replacement unit

PDR	Preliminary Design Review
PMA	pressurized mating adapter
PMBT	propellant mean bulk temperatures
PSD	Propulsion System Department
PRA	probabilistic risk assessment
PRL	Process Readiness Level
RAM	random access memory
RCS	reaction control system
Reqt	Requirement
RF	radio frequency
RQMT	Requirement
RTCA	RTCA, Inc. (formerly Radio Technical Commission for Aeronautics)
S	Standard
S-T	short transverse
SAE	SAE International (formerly Society of Automotive Engineers)
SBU	Sensitive But Unclassified
SDR	System Definition Review
SLS	Space Launch System
SMC	Space and Missile Systems Center
SOMD	Space Operations Mission Directorate
SP	Special Publication
SPEC	Specification
SRM	solid rocket motor
SRR	System Requirements Review
STD	Standard
STS	Space Transportation System
TBD	to be determined
Ti	titanium
TM	Technical Memorandum
TO	thrust oscillation
TP	Technical Paper
TPS	thermal protection system
TRL	Technology Readiness Level
TRR	Test Readiness Review
TVC	Thrust Vector Control
U.S.	United States
USAF	United States Air Force
UV	ultraviolet
Vdc	volt(s) direct current