Requirement: JPL Design Principles, Rev. 11

Effective Date: October 16, 2025

This information has been reviewed and approved for public distribution.

Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive
Pasadena, California 91109-8099

Table of Contents

1.0 Applicability and Introduction 8
1.1 Applicability 8
1.2 Introduction 8
1.3 Purpose 9
1.4 Organization 9
1.5 Compliance Assessment and Waivers 10
1.5.1 Compliance Assessment 10
1.5.2 Waivers 10
1.6 Scope of Requirements 11
1.7 Deviations and Exceptions 11
1.7.1 Reassessment after changes: Formulation and Implementation 12
1.7.2 Reassessment after changes: Operations 12
1.7.3 Non-compliances from reassessment 12
1.8 *Deleted* 12
1.9 *Deleted* 12
1.10 Mapping to Additional Rationale 12
2.0 Principles 12
2.1 Avoiding Impacts to Other Current or Future Missions 13
2.1.1 Enable Anomaly Investigations 13
2.1.2 Limit Risk Due to Orbital Debris and Reentry 13
2.1.3 Nuclear Material Considerations 14
2.2 Preventing Mission Failure 15
2.2.1 Mission Robustness 15
2.2.2 Avoidable Risks 15
2.2.3 Fault Protection Expectations 16
2.2.4 Life Test 16
2.2.5 Escapes 16
2.2.6 Test As You Fly 16
2.3 Mission Performance 17
2.3.1 Design for Ops 17
2.3.2 Unambiguous 17
2.3.3 Fault Avoidance 18
2.3.4 Cross-system effects 18

2.3.5 EMI/EMC 18
2.3.6 Graceful Degradation 18
2.3.7 Fault Recovery 19
2.4 Margins for Operations 19
2.4.1 Technical Resource Margins for Operations 19
2.4.2 Reliability through Design Margins 19
2.4.3 Robustness through Temperature Margins 20
2.5 Development/Implementation 20
2.5.1 Margins for Development 20
2.5.2 Avoid local optimization 21
2.5.3 Balance Performance against Risk 21
2.5.4 FOVs and Impingement 21
2.5.5 Test and analysis expectations 22
2.5.6 V&V Timing 22
2.5.7 ATLO Use Cases 22
2.6 Discipline Best Practices 22
2.6.1 Follow Identified Standards or Practices (possibly with JPL exceptions) 22
2.6.2 Follow Software Best Practices 22
2.6.3 Follow Telecom Best Practices 22
2.6.4 Follow Power/Pyro System Best Practices 23
2.6.5 Follow Control System Best Practices 23
2.6.6 Follow Separation and Deployment Best Practices 23
2.6.7 Follow Thermal Best Practices 23
3.0 Mission Design 23
3.1 General 23
3.1.1 Launch Period 23
3.1.2 Communications during mission - critical events 24
3.1.3 Protection of critical data 24
3.2 Mission Design Margins 24
3.2.1 Treatment of Statistical Delta 24
3.2.2 Treatment of Statistical Delta - 25
4.0 Flight System Design 25
4.1 General 25
4.1.1 Safety 25

4.1.2 Contamination 25
4.1.3 Design Robustness 25
4.1.4 Capturing diagnostic data during deployments or other critical dynamic events 27
4.1.5 Orbital Debris Limitation 28
4.1.6 Interfaces 29
4.1.7 Operability 29
4.1.8 *Deleted* 30
4.2 Mechanical Configuration/Systems Design 30
4.2.1 General 30
4.2.2 Configuration 30
4.2.3 Mechanisms 32
4.2.4 Mass Properties 38
4.2.5 Structural Design 38
4.3 Power/Pyrotechnics Design 43
4.3.1 General 43
4.3.2 Power Distribution 44
4.3.3 Power Generation 45
4.3.4 Pyrotechnic Function 50
4.4 Information System Design 52
4.4.1 General 52
4.4.2 On-board Processing 53
4.4.3 On-Board Storage 53
4.4.4 Commanding and Sequencing 54
4.4.5 Telemetry Modes and Formats 56
4.4.6 Telemetry Visibility 56
4.4.7 Timing and Synchronization 58
4.5 Telecommunications System Design 59
4.5.1 General 59
4.5.2 Command Links 60
4.5.3 Telemetry Links 61
4.5.4 Relay Links 61
4.5.5 Telecommunication System Margins 61
4.6 Guidance, Navigation & Control Design 62
4.6.1 General 62

4.7 Propulsion System Design 63
4.7.1 General 63
4.7.2 Sizing 64
4.7.3 Propulsion Design Margins 64
4.7.4 Safety 65
4.7.5 Propulsion Temperature Test Margins 65
4.8 System Thermal Design 66
4.8.1 *Deleted* 66
4.8.2 Temperature Control Design Performance 66
4.9 System Fault Protection Design 71
4.9.1 General 71
4.9.2 Fault Protection Response 73
4.9.3 Flight-Ground Interface 74
4.9.4 Fault Detection 76
4.10 System EMC/EMI Design 77
4.10.1 General 77
4.10.2 Grounding and Interfacing 78
4.10.3 Control of Emissions 79
4.10.4 Control of Susceptibility 80
4.10.5 Control of Electrostatic Discharge 81
4.11 Flight Software System Design 81
4.11.1 General 81
4.11.2 Initialization 83
4.11.3 Interfaces 84
4.11.4 Design Robustness 85
4.11.5 Verification 89
4.11.6 Diagnostic and Self-Test Capability 89
4.12 Flight Electronics Hardware System Design 90
4.12.1 General 90
4.12.2 Electronic Packaging 92
4.12.3 Digital Design 93
4.12.4 Analog Design 94
4.12.5 Interfaces 94
4.12.6 Flight Electronics Thermal Design 97

4.12.7 Power On/Off and Reset (POR) Design Considerations in Electronic Assemblies ... 98
4.12.8 Hazard Controls ... 99
4.12.9 Flight Hardware Margins - See 6.3.8 ... 99
4.12.10 Verification ... 100
4.12.11 Electro-mechanical ... 100
5.0 *Deleted* ... 100
6.0 Managed Margins ... 100
6.1 *Deleted* ... 100
6.2 Mission Design Resource Margins ... 100
6.2.1 Propellant ... 100
6.3 Flight System Technical Resource Margins ... 100
6.3.1 Alternative Margin Documentation ... 101
6.3.2 System Mass Margins ... 101
6.3.3 System Power/Energy Margins ... 106
6.3.4 *Deleted* ... 121
6.3.5 Flight Software Margins ... 121
6.3.6 Power/Pyrotechnic System Margins ... 122
6.3.7 Telecommunications System Margins ... 122
6.3.8 Flight Electronics Hardware Margins ... 123
6.3.9 S/C Mechanisms Functional Margins ... 123
6.3.10 Energy Margins for Cryogenic Systems ... 124
7.0 Flight Scenario Design ... 125
7.1 General ... 125
7.1.1 Operation Consistent with Flight Rules ... 125
7.1.2 Critical Event Telemetry Monitoring ... 125
7.1.3 Ground-in-the-loop Commanding ... 125
7.1.4 *Deleted* ... 125
7.1.5 Special Data Capture ... 125
7.1.6 Sequence Initial Conditions ... 126
7.1.7 Resource Margins for Stored Sequence Operations ... 126
7.2 Launch Scenario Design ... 126
7.2.1 Sequence End State ... 126
7.3 Trajectory Correction Maneuver (TCM) Scenario Design ... 126
7.4 Orbit Insertion Scenario Design ... 127

7.4.1 Sequence End State 127
7.5 Entry, Descent & Landing (EDL) Scenario Design 127
7.6 Aerobraking (A/B) Scenario Design 127
7.6.1 Exit Conditions 127
7.6.2 Aerobraking Aerostable Flight System Configuration 127
7.6.3 Aerobraking Thermal Margin 127
7.6.4 Aerobraking Required Operational Margins 127
7.6.5 Aerobraking Fault Protection Design 128
8.0 Flight System Verification and Validation Design 128
8.1 General 128
8.1.1 Minimum Operating Times for Electronics Assemblies 128
8.1.2 Handling and Test Constraints 130
8.1.3 Allocation and Tracking of Life Limited Items 130
8.2 Pre-delivery Verification 130
8.2.1 Subsystem and Assembly Level 130
8.2.2 Early Interface Testing 131
8.2.3 System Level 131
8.3 System Assembly, Integration and Test 131
8.3.1 System Assembly 131
8.3.2 System Integration 132
8.3.3 System Functional Verification 132
8.3.4 Flight Sequence Verification 135
8.3.5 System Fault Protection Verification 135
8.3.6 System Stress Testing 135
8.3.7 System Environmental Verification 135
8.3.8 Inter-System Verification 136
8.4 Launch Operations 136
8.4.1 Pre-mate Verification 136
8.4.2 Post-mate Verification 136
8.4.3 Launch-critical Support Equipment 137
9.0 Flight System Flight Operations Design 137
9.1 General 137
9.1.1 Communication during mission-critical events 137
9.1.2 Protection of critical data (Ref. DP 3.1.3) 138

9.1.3 Telecommunications availability for mission - defined special activities (Ref. DP 4.5.1.4) 138
9.1.4 Telemetry visibility of spacecraft state (Ref. DP 4.4.6.4) 139
9.1.5 *Deleted* 139
9.1.6 In-flight characterization (Ref. DP 4.1.7.2) 139
9.1.7 *Deleted* 139
9.1.8 Protection against errors (Ref. DP 4.1.3.2) 139
9.1.9 Stressing ground operations capability demonstration 140
9.2 Flight Software Operation 140
9.2.1 *Deleted* 140
9.2.2 Post-launch flight software update rigor and process 140
9.2.3 In-flight on-board flight parameter update 140
9.3 Flight Hardware Operation 140
9.3.1 Powering off the RF Downlink 140
9.3.2 Powering off the RF Receiver 141
9.3.3 *Deleted* 141
9.3.4 *Deleted* 141
9.3.5 *Deleted* 141
9.3.6 Simultaneous use of Prime and Redundant Hardware 141
9.3.7 *Deleted* 141
9.3.8 *Deleted* 141
9.4 Flight Scenario/Sequence Design 141
9.4.1 *Deleted* 141
9.4.2 Critical Event Telemetry Monitoring (Operations) (Ref. DP 7.1.2) 141
9.4.3 *Deleted* 141
9.4.4 *Deleted* 141
9.4.5 Special Data Capture (Operations) (Ref. DP 7.1.5) 142
9.4.6 Sequence Initial Conditions (Operations) (Ref. DP 7.1.6) 142
9.4.7 *Deleted* 142
9.4.8 *Deleted* 142
9.4.9 *Deleted* 142
9.4.10 *Deleted* 142
9.5 Operating Margins 142
9.5.1 Operating Margins for Real Time Operations 142

1.0 Applicability and Introduction

1.1 Applicability

This document applies to all persons participating in the design, verification/validation, and operation of flight systems intended for use in space.

The requirements of this document apply equally to spacecraft, payloads, instruments and Engineering Delivery Tasks (EDTs) . Note that some of these requirements have explicit differences between what is required for a Type I mission vs. a Type II or Type 0 mission; Type I, Type II, and Type 0 missions are generally defined as NASA class A, B, and C missions (Type I), NASA class D missions (Type II), and non-NASA missions (Type 0), with each of these tailored, based on JPL's past experiences.

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

All space flight projects managed by JPL are required to meet the requirements herein, or secure timely approval for any deviations/exceptions taken.

The requirements of this document are not required of flight system elements, provided to JPL, that are produced under the control of other NASA Centers, other government agencies, or by other nations. Voluntary application of the principles herein to these efforts is at the option of the JPL project on which these elements are manifested.

1.2 Introduction

This document specifies essential attributes of JPL space flight systems including aspects related to their design, verification/validation, and operation.

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

a. Incorporate lessons learned that were key to past successes, and where deviations created significant problems,
b. Capture the essence that contributes to JPL successes, including
    1. Robust design margins for high reliability
    2. Ample margins for management of development risk
    3. Comprehensive approach to flight system verification and validation, and

4. Conservative use of flight assets

c. Document the required flight design key attributes considering the uses to which the flight systems are put, and

d. Identify key attributes one discipline needs to provide to enable the success of one or more other system elements, and on which the system integrity is based.

The design principles herein do not attempt to represent the only design approach, rather specify the limits of risk-taking the institution is willing to accept before initiating discussion with the project- to understand the potential risks and the technical justification for their acceptance.

Certain requirements herein apply more broadly within a project than just the flight system. For example, some principles can only be met through cooperative efforts of mission design and flight system design.

1.3 Purpose

The purposes served by this document are to:

a. Define a set of design principles that communicate the character of JPL flight designs within JPL, and to industry and academic partners, and to the sponsor of these systems,

b. Establish a common standard by which project designs and risks can be assessed, and

c. Engage management in dialog, when deviations are taken, of the technical risks being assumed.

1.4 Organization

The convention used in organizing the document content is that principles are located with the discipline responsible for ensuring the principle is met. An exception is made for the principles arising from consideration of flight uses, which generate principles on flight design disciplines for the integrity of the flight scenario.

When a section is shown as "*Deleted*", the design rule has been retired. This document does not re-use numbers, so metrics may be easily tracked against each requirement across all projects.

The document is organized into six main sections:

1. Mission Design - section 3 contains principles that reflect on both mission design and flight system areas

2. Flight System Design - section 4 contains flight system design principles organized by functional area
3. Managed Margins - section 6 contains principles for managed margins pertaining to flight system technical resources
4. Flight Scenario Design - section 7 contains principles relating to the flight system uses in typical mission scenarios
5. Flight System Verification and Validation (V&V) - section 8 contains principles applicable to the flight system V&V activity
6. Flight System Flight Operations Design- section 9 contains principles applicable to the operation and in-flight maintenance of flight systems

1.5 Compliance Assessment and Waivers

Projects address compliance with the requirements herein at major reviews throughout the project life cycle.

The JPL Waiver System for Project and Institutional Requirements (WSPIR) tool is available to help mission and instrument projects record their state of compliance/non-compliance with the requirements ("**shall**") and guidelines ("should") herein.

1.5.1 Compliance Assessment

The initial documented compliance assessment addressing both requirements and guidelines **shall** be completed prior to the Preliminary Design Review (PDR) and captured in an inspectable product.

Note: *For Types 0, I and II projects, the compliance assessment for requirements and guidelines is captured in WSPIR.*

Note: *For all project Types (0, I, and II), the compliance assessment for requirements is reviewed by the Institutional Advisory Board (IAB).*

The Compliance Matrix is attached to the Project Implementation Plan (PIP).

1.5.2 Waivers

Requirement non-compliances **shall** be addressed via the Category A waiver process.

Technical justification is provided to support approval of requested deviations. This justification specifically addresses the risk associated with the proposed alternative to the requirement(s) contained herein.

Standard Category A waivers to JPL Design Principle requirements are approved by the applicable:

- Project Manager
- Engineering Technical Authority (ETA)
- Safety and Mission Assurance Technical Authority (SMA TA)
- Delivering Line Manager
- DP Document Owner
- Programmatic Manager
- Office of Safety and Mission Success (OSMS) Manager
- JPL Chief Engineer
- Associate Director for Flight Projects and Mission Success (AD FP&MS)

Streamlined Category A waivers are approved by a smaller subset of the list above; ETA, SMA TA, Delivering Line Organization, and DP Document Owner.

Disagreements among these parties are resolved by the Associate Director for Flight Projects and Mission Success.

1.6 Scope of Requirements

The Design Principles (DP) (this document) is an institutional requirement type document in the Directive category of institutional documents. Directive documents are required of those to which they apply. Applicability of the Design Principles is indicated in Section 1.0.

Requirements herein are identified through the use of "**shall**." Notes, Examples, and Rationale are explanatory, and do not contain any requirements. "*Should*" is used to describe a leading practice; such statements represent guidance rather than requirements.

Where a design rule points to standard or requirements documents, the latest revision of the document will be used.

1.7 Deviations and Exceptions

Note that alternative designs to those specified herein are not precluded, but require an approved waiver that includes the identification of the residual risk and the rationale as to the acceptability of the risk commensurate with the risk policy established by each project. Departures from established principles are controlled to ensure management awareness of and institutional involvement in project potential risk considerations.

Projects assess the requirements herein in the context of the specific mission application and project risk posture. Where the project evaluation suggests a deviation or exception to these principles is a prudent risk, the project presents

its case via waiver request, including the technical justification for the risk associated with the proposed alternative approach, to the appropriate authority for disposition of the request.

Requests for waiver to the requirements herein are made with adequate lead-time in case of disapproval.

Whenever a revision to the JPL Design Principles document is released, action is required from each project as indicated below:

1.7.1 Reassessment after changes: Formulation and Implementation

Projects in Formulation and Implementation phases **shall** assess and document their compliance with any new or revised requirements, as highlighted in the revised Design Principles Compliance Matrix publication.

1.7.2 Reassessment after changes: Operations

Projects in the Operations phase **shall** only assess and document their compliance with all operations-related changes.

1.7.3 Non-compliances from reassessment

Non-compliances **shall** be addressed through the Category A waiver process.

1.8 *Deleted*

1.9 *Deleted*

1.10 Mapping to Additional Rationale

A brief rationale is provided in this document where the justification for a design principle is not self-evident. Additional insight into the basis for a design principle may be gained from links inserted below the paragraph to lessons learned, the Design Principles Handbook, and other source material.

Note: *This mapping is maintained in part to ensure that when changes to the contents of this document are made they do not unknowingly un-do corrective actions taken to earlier problems or events.*

2.0 Principles

The majority of the design principle document is made up of statements that are requirements as in “The project **shall**…” or guidance as in “The project *should*…”. These can be described collectively as Design Rules (DR). They tell

engineers on a project what to do but are often missing a high level indication of the underlying principle that led to JPL writing down that design rule.

This section collects and captures those underlying principles with the intent that these principles will serve as the starting point for more extensive training material.

Each of the DRs maps to at least one of these principles. In some cases, a DR may map to multiple principles. Most but not all of the principles map to multiple DRs.

The principles are organized into six categories:

1. Avoiding Impacts to Other Current or Future Missions
2. Preventing Mission Failure
3. Mission Performance
4. Margins for Operations
5. Development/Implementation
6. Discipline Best Practices

Please note: The DP10 version of this principles section is a work in progress. For now, most principles consist of a sentence or two. The intent is for each principle to be expanded both here and in external training material so that they become valuable instructional material that provides context to the design rules that are connected to them.

2.1 Avoiding Impacts to Other Current or Future Missions

2.1.1 Enable Anomaly Investigations

Design and operate the mission in a way that assures that future anomaly investigations have the data needed to prevent future recurrence - even if the mission is lost.

Mapped to Design Rules: 3.1.2.1, 3.1.2.2, 4.1.4, 4.4.1.1, 4.4.5.3, 4.4.6.1, 4.4.6.8, 4.5.1.4, 4.11.2.4, 7.1.2, 9.1.1.1, 9.1.1.2, 9.1.3, 9.4.2.

2.1.2 Limit Risk Due to Orbital Debris and Reentry

Flight systems are designed and operated to limit the intentional generation of orbital debris around solar system bodies (excluding the sun) and their Lagrange points. Flight systems are also designed and operated to limit the human risk from Earth reentry.

Mapped to Design Rules: 4.1.5.1, 4.1.5.2, 4.1.5.3, 4.1.5.4, 4.2.3.7, 4.7.1.4.

2.1.3 **Nuclear Material Considerations**

Projects consider the full range of feasible options to assure mission success prior to baselining the use of nuclear materials for heat or power.

There should be a compelling engineering rationale for the use of nuclear material that is grounded in 'mission success' objectives that also have a sound scientific and/or engineering rationale. Baselining the use of nuclear material for thermal management or spacecraft power will require additional analyses and documentation to be developed by or on behalf of the mission, which may add schedule and cost considerations not otherwise encountered, and will include additional design considerations. Depending on the mission characteristics and type of nuclear material being considered, these efforts could include development or updating a launch vehicle databook to support a launch nuclear safety analysis, an interagency review process and in some cases Presidential approval for the launch, additional radiological contingency planning and preparations to support the launch, and risk communication support for the mission. Additionally, the mission would be required to support the development of documentation supporting NASA's National Environmental Policy Act (NEPA) compliance, and in some cases additional studies on the part of the mission would be required to support the rationale for use of nuclear material if other options are available. Involvement of the JPL Launch Approval Engineering Office early in the mission development phase will assure these additional requirements are identified, documented, and addressed.

When nuclear materials are baselined for heat or power, several technical considerations are added to the list of items the project must consider:

- The mechanical design and the propulsion design can affect the likelihood of release of radioactive material in the event of an at altitude or ground impact accident scenario. The location of hard points, concentrated masses, and propellants or pressurant tanks relative to a planned Radioisotope Power Source (RPS) or Radioisotope Heater Unit (RHU) location, or enclosure of the spacecraft within an aeroshell is thought through early in the system design.
- An accident that leaves the spacecraft stranded in orbit becomes an additional use case for the spacecraft Guidance, Navigation, and Control (GN&C) and other subsystems (e.g., sizing the spacecraft power system to allow the spacecraft to remain power positive after separation from the Launch Vehicle (LV) given a LV anomaly that leaves the spacecraft stranded in a low earth orbit). The system should plan to execute contingency plans to either boost to a higher earth orbit (A sufficiently high long-term storage orbit, consistent with debris mitigation policies, should allow for at least a 10-fold decay of radioisotopes) or to perform a controlled reentry consistent with orbital debris requirements if a high storage orbit cannot be accomplished.

- The use of solid propellant motors may warrant the addition of a breakup system to assure breakup of the solid motor material to reduce threats to RPS or RHU containment systems from solid propellant fire environments.
- Special attention is required to assure Earth impact probabilities are as low as reasonable, consistent with mission success and with NASA nuclear flight safety requirements. The spacecraft fault protection system is designed (i.e., leaves the spacecraft in a powered, commandable state with some thrust capability) such that given any orbital or post injection failures, the appropriate contingency actions can be taken.
- Pre-launch accidents (after integration of the RPS/RHU with the SC/LV stack) can be risk drivers for the overall safety assessment of the mission. The RPS/RHU integration timeline is determined early in the spacecraft design phase so that safety analysis of pre-launch accidents may proceed.

2.2 Preventing Mission Failure

2.2.1 Mission Robustness

Protect threshold mission in the presence of classes of flight system and mission system faults and operator errors.

For example, stored critical data is protected from loss, e.g., due to credible fault scenarios.

Mapped to Design Rules: 3.1.3, 4.1.3.1, 4.1.3.2, 4.3.1.1, 4.3.1.2, 4.3.2.1, 4.3.2.2, 4.3.2.3, 4.3.3.6.2, 4.3.3.7, 4.4.3.1, 4.4.4.4, 4.4.4.6, 4.4.4.7, 4.4.4.9, 4.9.2.3.1, 4.10.2.6, 4.12.1.6.2, 4.12.1.8.1, 4.12.5.6, 4.12.7.4, 4.12.8.1, 7.6.5, 9.1.1.3, 9.1.2.

2.2.2 Avoidable Risks

Design and operate the flight system to avoid exposure to known vulnerabilities.

Examples include:

- Developing a spacecraft configuration that attenuates the structural path shock transmission between pyrotechnic sources and sensitive components to levels that do not threaten to damage Spacecraft (s/c) hardware. Note: This includes the pyrotechnic events initiated by the launch vehicle as well as those controlled by the Spacecraft (s/c).
- Accommodating optics and other contamination sensitive components consistent with the sensitivity to, and the potential degradation from, particulate and molecular contamination. Note: This includes contamination originating from the launch vehicle as well as that attributable to s/c sources.

- Accommodating detectors and other Radio Frequency (RF) sensitive components in a manner to eliminate the potential for damage from spacecraft RF radiation sources.
- Assuring that the structural modes of all in-flight spacecraft mechanical configurations are compatible with the attitude control system design. This precludes structural resonances from adversely interacting with the spacecraft control systems. To accomplish this, primary and secondary structural modes within the attitude control bandwidth must be identified early and properly accounted for.
- Accounting for the systems effects (e.g., on stability, pointing, and fault protection) of propellant slosh dynamics, deployments, separations, and other sources of variability in spacecraft mass properties in the design and operation of the flight system.

Mapped to Design Rules: 4.1.3.5, 4.1.7.4, 4.3.4.3,4.4.3.2, 4.7.4.2, 4.7.4.3, 4.12.5.2.1, 4.12.5.7, 7.1.5, 8.1.2, 8.3.4.2, 9.3.2, 9.3.6, 9.4.5.

2.2.3 **Fault Protection Expectations**

Fault protection preserves flight system health, safety, and consumables throughout all mission phases, except when the completion of time critical events or activities takes priority.

Mapped to Design Rules: 4.9.1.2, 4.9.1.3, 4.9.1.4, 4.9.1.6, 4.9.1.7, 4.9.2.2, 4.9.2.2.2, 4.9.2.3, 4.9.4.1, 4.9.4.2.

2.2.4 **Life Test**

Verify minimum life margin for cycle or throughput-limited hardware and electronics.

Mapped to Design Rules: 4.2.3.9, 4.2.3.9.1, 4.2.3.9.2, 4.2.3.9.3, 4.7.3.1, 4.7.3.2, 4.7.3.3, 4.7.3.4.1, 4.7.3.4.2, 4.7.3.4.3, 4.12.2.1.

2.2.5 **Escapes**

Take actions during I&T and operations to detect errors and reduce the chance of escapes.

Mapped to Design Rules: 4.4.6.9, 4.12.5.4, 8.1.1.1, 8.1.1.2, 8.1.3, 8.3.1.1, 8.3.2.1, 8.3.2.2, 8.3.3.3, 8.3.3.5, 8.4.2.1, 9.1.8.

2.2.6 **Test As You Fly**

Test systems in conditions that match or exceed flight conditions and fly systems within the bounds that they have already been tested to.

Mapped to Design Rules: 4.1.3.4, 4.1.7.2, 7.1.1, 8.3.3.1, 8.3.3.2, 9.1.6.

2.3 Mission Performance

2.3.1 Design for Ops

Develop the project and flight system keeping operational impacts of design choices in mind.

Flight system design approaches that reduce operational complexity and interdependencies (e.g., require fewer calibrations, provide more on-board closed-loop control, provide robust technical margins, provide more autonomy) are strongly encouraged.

Examples include:

- Designing the on-board data storage to accommodate overall communications system performance needs, including requirements for return data volume, latency, priority, and quality.
- Designing the information system design to use adopted standards for ensuring reliable uplink of commands, sequences, and software loads.
- Providing visibility to support ground determination of the performance of s/c functions important to mission success.
- Ensuring that the update of critical flight software parameters is performed with the same rigor (review, testing, safeguards, operations procedures, etc.) as is applied for a full flight software update. Critical flight software parameters in this context means those that have a reasonable expectation of changing during the mission and that affect the nominal and/or fault protection performance of the spacecraft.

Mapped to Design Rules: 4.1.7.3, 4.3.3.5, 4.4.2.2, 4.4.3.3, 4.4.4.5, 4.4.4.6, 4.4.4.7, 4.4.4.8, 4.4.6.1, 4.4.6.8, 4.4.6.11, 4.5.1.1, 4.5.1.3, 4.5.4.1, 4.5.4.2, 4.9.3.1, 4.9.2.2.1, 7.1.3.

2.3.2 Unambiguous

Design the flight and ground systems to provide the ability to set and know the state of the flight system unambiguously.

Mapped to Design Rules: 4.2.2.15, 4.4.4.1, 4.4.4.2, 4.4.6.1, 4.4.6.4, 4.4.6.8, 4.4.7.2, 4.4.7.3, 4.4.7.4, 4.9.3.2, 4.9.3.3, 4.9.3.4, 4.9.3.5, 4.9.3.6, 4.9.3.7, 4.11.2.1, 4.11.2.2, 4.11.2.3, 4.11.4.14, 4.11.6.3, 4.12.3.2, 4.12.7.1, 4.12.7.2, 4.12.7.3, 7.1.6, 7.2.1, 7.4.1, 7.6.1, 7.6.2, 9.1.4, 9.3.1, 9.4.6.

2.3.3 **Fault Avoidance**

Take design action to avoid building-in known vulnerabilities.

Mapped to Design Rules: 4.4.3.4, 4.4.7.1, 4.8.2.4, 4.9.1.5, 4.11.4.2 (a, b, and c), 4.11.4.3, 4.11.4.11, 4.11.4.13, 4.12.3.1, 4.12.5.5.

2.3.4 **Cross-system effects**

Be aware of and limit undesirable cross-system or cross-subsystem interactions or their effects.

Mapped to Design Rules: 4.1.2.1, 4.1.2.2, 4.2.4.3, 4.7.1.3, 4.8.2.8, 4.12.2.3.

2.3.5 **EMI/EMC**

The grounding and interfacing design provides for an equipotential spacecraft. The design provides low conducted and radiated emissions, high transient noise immunity on circuitry, and magnetic field cancellation within each harness bundle. The design prevents (or minimizes) external and internal Electrostatic Discharge (ESD) and prevents Direct Current (DC) currents flowing through structure.

Mapped to Design Rules: 4.10.1.1, 4.10.1.2, 4.10.2.1, 4.10.2.2, 4.10.3.1, 4.10.3.2, 4.10.3.3, 4.10.3.4, 4.10.4.1, 4.10.4.2, 4.10.4.3, 4.10.4.4, 4.10.4.5, 4.10.5.1, 4.10.5.2

2.3.6 **Graceful Degradation**

To reduce the possibility of catastrophic mission loss or major mission degradation, build design robustness through graceful degradation following a failure. Graceful degradation refers to an incremental loss of functional capability following a failure, such that a reduced set of mission requirements is still being met, and there is still significant mission return.

Design robustness includes consideration of:

a. Inadvertent operation outside expected flight environments, e.g., temperatures, radiation dose
b. Shortfalls in performance, e.g., RF power output, antenna gain
c. Alternative methods for achieving necessary objectives, if a failure occurs in flight.

Mapped to Design Rules: 4.8.2.5, 4.11.4.6, 4.11.4.7, 4.11.5.4.

2.3.7 **Fault Recovery**

Full mission capability is retained or recovered following faults or operator errors.

Mapped to Design Rules: 4.3.3.4, 4.11.4.5, 4.12.1.1, 4.12.1.6.1.

2.4 Margins for Operations

2.4.1 **Technical Resource Margins for Operations**

Provide flexibility in flight operations by preserving a portion of the technical resource margins at launch to solve problems that come up after launch.

Margins in technical resources such as power/energy, memory, bus bandwidth, computational throughput, and delta-V provide for additional flexibility to accommodate changes in the flight operational phase, e.g., if differences from predicted conditions are encountered.

Mapped to Design Rules: 4.3.3.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.8, 6.3.3.3, 6.3.5.3, 7.1.7, 9.5.1.

2.4.2 **Reliability through Design Margins**

Design margins are established consistent with design maturity and mission environments, and to allow for potential changes to environment and mission/system design requirements, as well as for surprises from "unknown unknowns". A portion of these margins are retained beyond design completion for the flight operations phase. These margins are met under worst-case conditions and end of life, unless otherwise specified.

Robust margins enable design and programmatic trades to be made effectively and rapidly without lengthy studies, thereby preserving programmatic resources (budget and schedule). Robust margins also allow design changes to be made with minimal system-wide “ripple” effects.

Margins exist to cover uncertainties in performance capability as predicted via analysis and/or modeling. To the extent that the uncertainties assumed during the design over-bound the flight conditions, design margins provide excess capability that can be used in flight operations, e.g., higher data rates on the telecom links, less settling time after perturbing the spacecraft (s/c) pointing. Design margins (e.g., cycle life margins) also exist to provide confidence in the design to meet the performance requirements. These margins are not available for nominal flight operations, but may be used in responding to anomalies.

Mapped to Design Rules: 4.2.3.1, 4.2.3.3, 4.2.3.5.1, 4.2.3.5.2, 4.2.3.6, 4.2.5.2, 4.2.5.3, 4.2.5.4, 4.2.5.5, 4.2.5.6, 4.2.5.8, 4.2.5.10.1, 4.2.5.10.2, 4.7.3.5.1, 4.7.3.5.2, 4.8.2.10, 4.8.2.11, 4.12.1.5, 4.12.1.8.3, 7.6.4.

2.4.3 Robustness through Temperature Margins

Temperature margins are established and demonstrated to assure performance beyond expected flight temperature ranges to provide robustness in the case of a thermal surprise in flight or a recoverable fault.

Mapped to Design Rules: 4.2.3.12, 4.2.5.7, 4.7.5.1, 4.7.5.2, 4.8.2.3, 4.8.2.6, 4.8.2.7, 4.8.2.12, 4.8.2.13, 4.12.6.1, 4.12.6.2, 4.12.6.3, 4.12.6.4, 4.12.6.5, 7.6.3.

2.5 Development/Implementation

2.5.1 Margins for Development

Manage development risk through establishment of margin or use of performance parameters that contain margin. In some cases, the appropriate margin is a function of project lifecycle phase.

Technical resources include any quantifiable, bounded system characteristic for which the demand or need may exceed the capability. The available capability can be externally imposed, such as launch vehicle lift capability, or internally derived, such as solar array generation, data storage capacity, propellant, etc. Mass and power are the most common constrained resources for aerospace applications.

Designing systems with significant new elements brings with it inherent uncertainties. Establishing and managing margins is a key method for maximizing the probability that the finished system will be able to meet the resource constraints and demands.

For certain types of technical resources (e.g., mass and power) the required margin can be reduced as the design matures and uncertainty decreases. These resource margins can be thought of as being consumed along a pre-planned glide slope during development. For other types of technical resources (e.g., pointing and stability margins) the margin is established once and not consumed during development, although even in these cases there may be explicit control of decreasing uncertainty using other characteristics (e.g., a model uncertainty factor which decreases over time to reflect the increasing fidelity of a model).

In many cases, a resource will be divided into allocations, which allows the margin to be managed in separable design activities, often by systems engineers within different offices or elements of the Project.

Ample s/c technical margins should exist at the outset and throughout the development to be able to complete the development with acceptable residual risk to the mission, and present to the flight team at launch a system that is, if not easy to operate, then at least operable with acceptable risk.

Ample margins in technical resources together with budget reserves and schedule margin provide for the management of risk. When these resources are plentiful, options are readily available for resolving development and operational issues. When these resources are inadequate, finding acceptable solutions to problems is made more difficult, is more time-consuming, and can result in a system design that either is difficult to operate and thus error-prone, or is not as robust to random failures as prudent design- based on past experience would dictate.

Mapped to Design Rules: 4.3.3.2, 4.3.3.5, 4.7.2.1, 4.7.2.2, 6.3.2.3, 6.3.2.5, 6.3.3.3, 6.3.3.5, 6.3.5.3, 6.3.6.1, 6.3.6.2, 6.3.7.1 (.a and .b), 6.3.8.1, 6.3.9.1, 6.3.10.1, 7.6.4.

2.5.2 **Avoid local optimization**

The number and type of interfaces employed in the design are constrained to avoid duplication of design and testing effort when assessed at the system level.

For example, system designs using identical electrical interface design for interfaces that have common requirements and protocols can avoid duplication of effort across the project.

Mapped to Design Rules: 4.1.6.3.

2.5.3 **Balance Performance against Risk**

Attempting to reduce risk to very low levels can have a substantial impact on the nominal mission performance. In such cases, find a balance achieving acceptable risk and acceptable performance.

Mapped to Design Rules: 3.1.1, 3.2.1, 3.2.2.

2.5.4 **FOVs and Impingement**

Configuration design accommodates sensor and antenna Field of Views (FOVs) and thruster impingement.

Examples include direct and stray light FOV for attitude control celestial reference sensors and science imaging instruments.

Mapped to Design Rules: 4.2.2.5, 4.2.2.6, 4.2.2.7.

2.5.5 Test and analysis expectations

For certain components or configurations, test cases are explicitly defined or design cases are explicitly defined implying required test or analysis cases.

Mapped to Design Rules: 4.2.3.10, 4.2.3.10.1, 4.2.3.10.2, 4.2.3.11, 4.7.1.2, 4.12.3.3, 8.3.3.4, 8.3.3.8, 8.3.4.1, 8.3.5.1, 8.3.6.1.

2.5.6 V&V Timing

Certain verification and validation actions are scheduled prior to or during a specific event.

Mapped to Design Rules: 8.2.1, 8.2.2, 8.2.3, 8.2.3.1, 8.2.3.2, 8.3.3.6, 8.3.7.1, 8.3.7.2, 8.3.8.1, 8.3.8.2, 8.4.1.1, 9.1.9.

2.5.7 ATLO Use Cases

Consider each of the Assembly, Test, and Launch Operations (ATLO) use cases in the system design.

Mapped to Design Rules: 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.9, 4.11.1.4, 4.11.6.1, 4.11.6.2, 4.12.1.8.2, 4.12.5.1, 4.12.5.1.1, 4.12.5.2, 4.12.5.3, 4.12.8.1, 4.12.8.2, 4.12.10.1, 8.1.3, 8.4.3.1, 8.4.3.2.

2.6 Discipline Best Practices

2.6.1 Follow Identified Standards or Practices (possibly with JPL exceptions)

Mapped to Design Rules: 4.1.1, 4.1.3.6, 4.2.5.1, 4.2.5.8, 4.2.5.9, 4.7.1.1, 4.8.2.9, 4.11.3.1, 4.12.3.4.

2.6.2 Follow Software Best Practices

Mapped to Design Rules: 4.11.1.1.1, 4.11.1.1.2, 4.11.1.3, 4.11.1.5, 4.11.3.3, 4.11.4.12, 4.11.5.2, 9.2.2, 9.2.3.

2.6.3 Follow Telecom Best Practices

The telecommunications system (end-to-end flight and ground telecom elements) is designed to meet the required information return, radio navigation and, when applicable, radio science requirements.

Mapped to Design Rules: 4.5.2.1, 4.5.3.1, 4.5.5.1.

2.6.4 Follow Power/Pyro System Best Practices

Mapped to Design Rules: 4.3.3.3, 4.3.3.6.1, 4.3.3.6.1.b, 4.3.3.6.1.c, 4.3.4.1, 4.3.4.2 (& .a, .b, .c), 4.3.4.4, 4.3.4.5, 4.12.11.1

2.6.5 Follow Control System Best Practices

Mapped to Design Rules: 4.6.1.2, 4.6.1.3, 4.6.1.4.

2.6.6 Follow Separation and Deployment Best Practices

Mapped to Design Rules: 4.2.2.8, 4.2.2.12, 4.2.3.4, 4.2.3.8.

2.6.7 Follow Thermal Best Practices

The thermal control design is tailored to the specific applications of the mission, with consideration for both equipment reliability and temperature/performance interactions. The impact to the thermal design from credible failure modes is assessed.

Mapped to Design Rules: 4.8.2.9.

3.0 Mission Design

3.1 General

3.1.1 **Launch Period** - The launch period **shall** (**not** required for Type II, *should* for Type 0) be of sufficient duration to provide a probability equal to or greater than 99% of the countdown reaching T−0. In the absence of sufficient launch vehicle history and other data relevant to the project's launch plans to justify a statistical analysis, there **shall** (**not** required for Type II, *should* for Type 0) be launch opportunities on at least 20 different days, although the days need not be consecutive.

Rationale: The 20 days originated from an analysis of launch vehicles that are no longer in use. (The analysis was from Delta launches from 1989 to 2001.) Subject matter experts still judge it to be an appropriate value to provide the required probability in the absence of sufficient data to estimate a better value for the project. In addition to launch vehicle history, other data that may be applicable include the probability of weather that could cause delays for the time of year or time of day of the launch.

3.1.2 **Communications during mission - critical events**

Note: *Mission-critical events are those that if not executed properly and in a timely manner could result in failure to achieve mission success, e.g., orbit insertion; entry, descent, and landing. A Trajectory Correction Maneuver (TCM) is not mission-critical unless it must execute properly in the time scheduled for it, i.e., cannot be delayed.*

Note: *Protection against loss of unique data, e.g., one-time science is covered in 3.1.3.*

3.1.2.1 **Uplink/Downlink capabilities** - The mission design **shall** (*should* for Type II and Type 0) provide for a real time downlink capability during mission critical events.

Note: *Communications during other special mission events is addressed in 4.5.1.4.*

3.1.2.2 **Redundant spacecraft to ground data paths** - The mission design **shall** (*should* for Type II and Type 0) ensure that no single failure results in loss of return of flight data from mission critical events.

Note: *Scheduling of mission critical events to occur during the overlap of 2 tracking complexes is one way to satisfy this requirement. A direct-to-earth link to one tracking complex, plus an Ultra High Frequency (UHF) link to an orbiting asset that relays the data to another tracking complex is another way to satisfy this requirement.*

Note: *It is recognized that Earth-orbiting missions generally do not have events (other than the launch sequences) that fit the criteria for being mission-critical.*

3.1.3 **Protection of critical data** - The mission design **shall** ensure that recovery of science and/or engineering data deemed critical to mission success not be dependent upon the availability of a single tracking complex.

Note*: Applicability is post-launch data essential to mission success.*

Note*: On-board storage for later (re)transmission to Earth provides protection against loss of the real time link.*

3.2 Mission Design Margins

3.2.1 **Treatment of Statistical Delta** - V Estimates - Statistical delta velocity estimates **shall** (**not** required for Type II or Type 0) be based on 99% probability.

3.2.2 **Treatment of Statistical Delta -** V Estimates - For Type 0, statistical delta velocity probabilities **shall** be negotiated with the sponsor and specified in the Project Plan.

4.0 Flight System Design

4.1 General

4.1.1 **Safety** - All elements of the flight system **shall** adhere to the applicable design requirements of JPL Standard for System Safety.

4.1.2 **Contamination**

4.1.2.1 **Molecular contamination** – When degradation of essential functions by molecular contamination may jeopardize mission success, the design **shall** include in-flight methods, e.g., flash heaters, to mitigate the threat.

4.1.2.2 **Contamination covers** – Mission-critical optics **shall** be equipped with contamination covers that are removed (jettisoned, released, deployed) in flight, unless the contamination analysis demonstrates that contamination from flight and ground sources is not a threat.

4.1.3 **Design Robustness**

4.1.3.1 **Single failure tolerance** - No single failure of any electrical, mechanical, optical, or electromechanical element **shall** result in a failure to meet the threshold mission requirements (i.e., all Crit-II functions per the FPP definitions).

Note: *All Single Point Failures (SPFs) must be identified. Potential SPFs may be permitted if the risk is mitigated by appropriate preventive measures and sufficient technical rationale exists that indicates a low likelihood of failure.*

Note: *The purpose of this redundancy requirement is to protect threshold mission outcomes in the presence of many classes of failures. For example, these include random component failures, operations or environment errors that damage or degrade functions, and some classes of design errors where the cause of the first error can be mitigated using redundant elements. It is understood that redundancy is not a panacea to mitigate risk (and in some cases redundancy is not physically possible). However, where it is not used, there needs to be solid, well-considered, rationale (documented in waivers to this requirement), and those decisions need to be understood by management and clearly communicated to customers.*

Generally, this redundancy requirement is intended to be applied above and beyond any duplicative hardware needed to meet the lifetime requirements.

Criticality II (Crit-II) functions on Type I missions (those that are required to meet the project's threshold requirements) might include engineering subsystems like command and telecom, thermal, power, and many others. For Type I missions featuring a monolithic science instrument, this requirement insists that some form of block or functional redundancy be applied on the science measurement system (e.g., requiring separate vertical and horizontal channels on an imaging radar).

Note also that regardless of mission type, Criticality I (Crit-I) functions (those functions required to meet human health and property or environmental damage avoidance requirements) may require more than single fault tolerance (i.e., typically two or more fault tolerance depending on the risk).

4.1.3.2 **Protection against operator errors** - The design **shall** protect against ground operator errors that could result in loss of mission or significant impact to operations.

Example: requiring an enable command prior to actuation of a potentially hazardous command, including mode dependent lockouts and fault protection that corrects manageable classes of operator errors.

Note: *The intent is to minimize overall mission risk.*

4.1.3.3 ***Deleted***

4.1.3.4 **Commissioning/test of redundant/backup hardware** - The mission plan, operations plan, and flight system **shall** be designed, verified, and validated to enable a safe and reliable commissioning/test and, if applicable, calibration of redundant/backup hardware considered part of the mission success strategy, including critical events.

Rationale: This encourages early verification of readiness of hardware/software for mission-critical activities, allows for the confirmation of redundancy availability to support fault recovery activities, and permits the system to be safely debugged in advance if there are any issues.

Note 1: *Following stressing events (such as launch), implementing commissioning activities of redundant/backup hardware enables*

the early verification of hardware and software readiness to deal with future fault threats.

Note 2: *The test and calibration of redundant/backup hardware should be done without reconfiguration of the prime hardware, if possible.*

4.1.3.5 **Motor reversibility** - The flight system **shall** implement the capability to reverse motor direction in flight, even if only unidirectional motion is nominally required during the mission.

Rationale: Reversing motor direction is a key mitigation to aid recovery efforts for a jammed mechanism during the mission. This is a Lessons-Learned from Galileo, where the high gain antenna motors could not be reversed for attempts to unjam the deployable reflector.

4.1.3.6 **Parachute systems** – Parachute systems **shall** be designed and procured according to the requirements of Parachute Systems and Softgoods.

4.1.4 **Capturing diagnostic data during deployments or other critical dynamic events** – For Crit-II deployments, projects ***should*** collect sufficient data to allow them to understand completeness of deployment and to support recommendations for actions in response to incomplete deployment. Other critical dynamic events ***should*** be considered for similar data collection. Crit-II is defined as a failure to meet one or more Level 1 threshold (floor) requirements for the mission.

Note: *This design rule might, for example, be satisfied via visual recording of the deployment using a "do-no-harm," off-the-shelf camera or high-bandwidth recording of Inertial Measurement Unit (IMU) data or motor currents.*

Note: *This design rule is intended for the direct troubleshooting of potential deployment problems and for the development of lessons learned for mechanism design for future Missions.*

Rationale: Visual verification systems have proved a valuable tool for understanding Mars 2020 Entry, Descent, and Landing (EDL) as flown, and high-bandwidth IMU data were valuable in understanding the Soil Moisture Active Passive (SMAP) deployment. One can infer that similar capability may have provided useful data to diagnose past deployment anomalies, such as Galileo, Magellan, Mars Global Surveyor, and Lucy. Surface Water and Ocean Topography (SWOT) has already made a decision to add Mars 2020-like Commercial, Off-

the-Shelf (COTS) cameras to observe critical deployments. There is no expectation of real-time transmittal of this data.

4.1.5 Orbital Debris Limitation

4.1.5.1 **Limiting intentionally-released orbital debris** - Flight systems **shall** be designed and operated to limit the intentional generation of orbital debris around solar system bodies (also Lagrange points, and excluding the sun.)

Note: *For example, the use of bolt catchers and retained covers on Earth orbiters, and timing of jettisoned covers on planetary missions are methods by which to limit orbital debris.*

4.1.5.2 **Limiting unintentional and end-of-mission orbital debris** - The design and flight operations of Earth, Moon, and Lagrange Point-orbiting flight systems **shall** employ designs that limit the likelihood of unintentional generation of debris during and after the mission (e.g., use of spacecraft structure to protect pressure vessels from debris impact, propellant depletion burns at end-of-mission to eliminate on-board stored energy).

Rationale: Removal of stored energy at end of mission precludes it from creating or exacerbating a scenario in which a break-up of the spacecraft occurs. For example, catastrophic rupture of a tank of hydrazine is initiated by debris impact, transforming the spacecraft from one large piece of debris into many smaller but still dangerous pieces of debris. (Impact by an aluminum object roughly the size of a softball would completely break up a spacecraft. Impact by a centimeter-sized object could easily disable a spacecraft.)

4.1.5.3 **End-of-mission capability** - Earth-orbiting flight systems **shall** be designed with the capability to be safely and reliably de-orbited, or moved to a safe storage orbit at the end-of-mission. (Reliability considerations include hardware reliability, the possibility of an explosion or other break-up, and debris impact that would disable the spacecraft.)

Note: *De-orbit can be by active maneuver and/or natural orbit decay.*

Rationale: By limiting the amount of time that an abandoned space vehicle remains on orbit, we limit the chance that it will collide with another large object and generate a large amount of debris.

4.1.5.4 **Limiting human casualty risk from reentering debris** - For end-of-mission disposal by reentry into Earth's atmosphere, the flight system components estimated to survive reentry **shall** pose an acceptable risk of human casualty. as defined in Orbital Debris Assessment and Mitigation.

Note: *The casualty risk requirement is best met by avoiding the use of titanium and tungsten. It is acceptable to use a material other than titanium for adequate, rather than ideal, design implementation and performance. Where volume constraints permit, brass would be the preferred substitute for tungsten in balance mass, because brass will demise on reentry.*

4.1.6 Interfaces

4.1.6.1 ***Deleted***

4.1.6.2 ***Deleted***

4.1.6.3 **Use of proven interface types** - The system design *should* use proven reliable interface types where fault issues, etc. have already been addressed, e.g., 1553 data bus or other avionics standards.

Rationale: Minimizes implementation risk.

4.1.7 Operability

4.1.7.1 ***Deleted***

4.1.7.2 **Design for in-flight characterization** - The flight system design *should* provide accommodation(s) for early in-flight demonstration of spacecraft functional capability that may be performed prior to the actual mission need in order to characterize and evaluate the spacecraft and ground system end-to-end operation.

Note: *Early characterization/evaluation enables the project to identify flight/ground system shortfalls, and make changes safely and reliably with minimal threat to the mission.*

4.1.7.3 **In-Flight Reprogrammability** - For all elements that were reprogrammable at the assembly level, the system **shall** support and demonstrate the ability to reprogram those elements utilizing only available interfaces in the flight configuration.

Note: *This principle applies to reprogrammable elements resident in the main spacecraft computer, the on-board instruments, and any*

spacecraft assemblies containing reprogrammable flight software or hardware, such as star trackers, Electra UHF transceiver, etc. This includes through the RF interface and on the pad through the launch umbilical.

4.1.7.4 **Missed contact with the ground** - During non-critical spacecraft operations, the design and operation of the spacecraft **shall** ensure that it remains safe and operable for a minimum duration of at least twice the maximum interval between planned ground contacts.

Rationale: A missed uplink should not result in the need to declare an emergency, thereby disrupting scheduling of tracking resources.

Note: *The spacecraft should accommodate no ground contact for at least 2 weeks during interplanetary cruise.*

4.1.7.5 ***Deleted***

4.1.8 ***Deleted***

4.2 Mechanical Configuration/Systems Design

4.2.1 General

4.2.1.1 ***Deleted***

4.2.2 Configuration

4.2.2.1 **Accessibility** - The design **shall** provide accessibility for:

a) assembly/disassembly, handling, and transportation,

b) testing and troubleshooting, including alignments, and calibrations, and

c) maintenance and servicing in the planned ground operations flow including integrated operations with the launch vehicle

4.2.2.2 **"Blind" connectors** - The design **shall** avoid use of electrical connectors that require a blind mating in system level assembly, test and launch operations.

Note: *"Blind" mating refers to the lack of a clear view of the connection being made by the person making the connection.*

4.2.2.3 **Sharp edges** - Flight equipment corners and edges that represent a potential hazard in handling, assembly, and testing **shall** be designed to preclude injury to personnel and damage to flight hardware that otherwise might occur as a result of snagging of the garments worn by technicians working on the system.

4.2.2.4 ***Deleted***

4.2.2.5 **Venting** – When a spacecraft requires venting of gas or liquid, the potential for contamination, forces, or moments due to the vented material impinging on spacecraft surfaces **shall** be evaluated for accommodation in the configuration design.

4.2.2.6 **Plume impingement** - Thruster plume impingement *should* be precluded.

Note: *A nominal 45-degree half-cone angle is a typical thruster plume exclusion zone for chemical propulsion thrusters to avoid excessive impingement forces and torques, although this guideline may not be adequate to address contamination hazards.*

Note: *For electric propulsion thrusters, a nominal 90-degree half-cone exclusion zone should be considered for acceptable levels of sputter erosion and impingement forces and torques, although this guideline may not be adequate to address redeposition, thermal flux, and possible electron current collection.*

4.2.2.7 **RF pattern distortion** - The configuration design **shall** provide a clear view to the antenna aperture throughout the range of angles, relative to the boresight, that is required for telecommunications capabilities planned throughout the mission.

Rationale: Minimize RF antenna pattern distortion effects and multi-path reflections.

4.2.2.8 **Appendage deployments and separations** - Launch retention features and separation devices **shall** be aligned with the first motion vector of spacecraft appendage deployments at the interface of mechanical release.

Rationale: Minimize transverse motion at a separation joint.

4.2.2.9 **Design deployables for test** - Wherever practical, appendages and other deployables **shall** be capable of deployment under Earth-gravity conditions without off-loading by ground support equipment. When it is not practical to design for unassisted deployment (e.g., large

appendages), the initial design **shall** incorporate appropriate interfaces for gravity off-load ground support equipment.

Rationale: In order to allow the best validation during system testing, it is desirable for hinge bearings and cantilevered structure to be capable of sustaining gravity loading. Consideration should be given to the planned spacecraft or instrument orientation relative to gravity during environmental testing, where vertically orientated hinge-lines could allow unassisted deployment.

4.2.2.10 ***Deleted***

4.2.2.11 ***Deleted***

4.2.2.12 **Clearances** - The design **shall** ensure positive non-contacting clearances during launch dynamics and no recontact for all separations, deployments, releases, jettisons, and articulations under nominal and 3-sigma or worst-case conditions.

4.2.2.13 ***Deleted***

4.2.2.14 ***Deleted***

4.2.2.15 **Deployment Telemetry** - Deployable appendages, and any deployable that has a significant effect on the flight system mass properties, **shall** provide direct telemetry (such as a microswitch) to indicate the flight system configuration.

Note: *All deployment events that change the flight system configuration are to be telemetered to be consistent with Section 4.4.6 and paragraphs 4.5.1.4, 9.1.3 and 9.1.4 of this document. When the deployable exhibits insignificant mass property changes (as approved by the flight system and attitude control subsystem), indirect secondary telemetry can be allowed for the mission operation such as proper instrument function or detectable temperature change.*

Rationale: This paragraph emphasizes JPL telemetry requirements within the Mechanical Section of this document, to ensure proper implementation for flight mechanical systems.

4.2.3 Mechanisms

Note: *Mechanism functional Force and Torque Margins are defined as:*

Force Margin = { [(min. force available) / (max. force required)] -1} * 100

Torque Margin = { [(min. torque available) / (max. torque required)] -1} * 100

4.2.3.1 **Deployment systems design margin** - Mission critical deployment and separation systems (e.g., solar arrays and other spacecraft appendages, spacecraft-to-launch vehicle separations, etc.) **shall** demonstrate a functional force or torque margin of at least 100% for the entire range of motion.

Note: *The margin applies under worst-case conditions, including restart from any position within the range of motion including incipient latching events.*

Verification: *by testing under environmental conditions and supporting analysis, paying particular attention to quantifying worst-case force/torque losses due to cold, stiff cable bundles, the potential range of the coefficient of friction, and vacuum versus air effects.*

4.2.3.2 ***Deleted***

4.2.3.3 **Actuator design margins** - Mission critical mechanisms and actuators (e.g., electromechanical motors and solenoids, phase-change and state-change actuators, piezoelectric and electrostrictive devices, and spring-energized devices, or mechanisms driven by these devices) **shall** demonstrate at least 100% torque/force margin for the entire range of motion.

Note: *The margin applies under worst-case conditions at the end-of-life, including restart from any position within the range of motion.*

Note: *For piezoelectric devices, the depoling force limit is to be considered the device's ultimate strength for stress margin analysis.*

Verification: *by testing under environmental conditions for beginning of life conditions, supported by test and/or analysis for end of life conditions.*

4.2.3.4 **Use of kick-off springs for assured first motion** - Kickoff springs (also called "helper" or "separation" springs) **shall** be used to assure first motion for all in-flight separation joints.

Note: *An exception for the usage of kickoff springs in an in-flight separation joint is for entry, descent and landing systems, where*

combined forces from the descent parachute and gravity provide substantially more separation force than the implementation of any practical spring design.

Verification: by design review, analysis, and/or test.

4.2.3.5 **Spring Design Requirements**

4.2.3.5.1 **Mission-Critical Preloaded Springs** - Preloaded springs that are mission-critical for function **shall** be designed for positive stress margin at maximum preload using a factor of safety of 1.50 to yield and 1.65 to ultimate strength.

4.2.3.5.2 **Safety-Critical Preloaded Springs** - Safety-critical preloaded springs, that are not constrained from hazardous release of material should failure occur, **shall** be designed for positive stress margin at maximum preload using a safety factor of 1.65 to yield and 2.00 to ultimate strength.

Note: *Caution: Preloaded springs often must be compressed more than the designed preload during installation. Consideration should be given by the design engineers to not overstress the springs during installation, using a factor of safety ≥ 1.0 for the compressed height at installation.*

4.2.3.6 **Stroke margin for linear actuators** - Linear actuator output devices utilized for mission critical mechanisms **shall** demonstrate at least 10% stroke margin above the input stroke requirements of the mechanism. That is, the linear actuator output stroke capability **shall** provide 110% of the required input stroke to the mechanism to perform the mechanism function.

Note: *Examples of linear input motion actuator devices are paraffin actuators, solenoids, and shape-memory metal devices.*

Note: *The margin applies under worst-case conditions at the end-of-life.*

Verification: By testing under environmental conditions for beginning of life conditions, supported by test and/or analysis for end of life conditions.

4.2.3.7 **Bolt catchers for pyrotechnic separation nuts** - Where pyrotechnically-actuated separation nuts are utilized in the flight system, bolt catchers **shall** be incorporated in the design to ensure that the bolt is contained.

Note: *It is also recommended to incorporate energy absorption features (such as crushable honeycomb) within the bolt catcher housing.*

Rationale: Limit orbital debris and the necessity to perform separation analyses for the bolt. Assure that ejected bolts do not threaten personnel safety.

4.2.3.8 **Spring energized bolt release for actuated separation nuts** - Where actuated separation nuts are utilized in the flight system, a spring **shall** be incorporated in the design to ensure positive retraction of the bolt from the separation interface. The spring stroke **shall** meet or exceed the bolt stroke necessary for complete withdrawal of the bolt from the separation interface.

4.2.3.9 **Mechanisms cycle life testing** -

Mission Critical mechanisms that function in a cyclic manner, and one-time usage deployment mechanisms, **shall** demonstrate a minimum life capability according to Table 4.2.3-1.

Rationale: This requirement defines life testing of flight moving mechanical assemblies consistent with JPL heritage qualification practices.

Table 4.2.3-1 - Mechanisms cycle life design margins

Mission Critical Mechanism Element Type	Minimum Cycle Life Margin Requirement
Wet-lubricated low friction elements (e.g., rolling element bearings, involute gearing, etc.)	100%
Dry-lubricated elements, and wear-life limited elements (e.g., brush motors, slip rings, worm gearing, acme screw nut, etc.)	200%
Wet-lubricated low friction elements, operating below the temperature rating of the lubricant	200%
Flexure pivots and suspension elements, bending cycle life (fatigue)	200%
Magnetic bearings and pressurized fluid bearings, touchdown events from startup and power-down	200%

Verification: By life test of a Qualification unit, incorporating nominal ground test and mission cycle requirements, with a portion of the life test performed under worst-case environmental conditions. (A guideline for the life test is 50% of the cycle life test under nominal temperature conditions, with 25% at Qual cold and 25% at Qual hot temperature conditions.)

Note: *Qualification Cycle Life Test Margin is defined as:*

Qualification Cycle Life Test Margin (%) = {[(cycles demonstrated by life-testing of a qual unit) / (ground test cycles planned for flight unit + flight operational cycles)] -1} * 100

There is no defined Cycle Life Test Margin for a one-time deployment mechanism in a Protoflight (PF) program.

4.2.3.9.1 **Mechanism cycle life design margin** - The mission critical mechanism **shall** operate within specified performance at the end of the life test as conducted according to Table 4.2.3-1.

4.2.3.9.2 **Disassembly and Inspection** - The life-test unit **shall** be disassembled and inspected for unacceptable wear or debris generation. Radiological evaluation such as Fein-focus X-ray, CT X-ray or N-ray may be utilized instead of destructive disassembly for sealed systems (Stirling pumps, cryo-coolers, sealed pumps, propulsion valves, etc.) as long as the resolution is adequate for assessment of wear, dimensional changes and wear-debris.

4.2.3.9.3 **One-Time Deployment Mechanisms** - One-time deployment mechanisms may be verified within a PF program as long as inspections and other technical metrics are implemented to verify the post-life test condition of the hardware, and adequate testing of the deployable hardware after final assembly is performed. The protoflight ground test verification for a one-time deployable mechanism **shall** be at a minimum of four operations, defined as once at ambient temperature, once at PF hot bound, once at PF cold bound, and once in System Test on the flight system. (System testing may be limited to “first motion” actuations for large appendages.) The maximum protoflight ground test cycles, to avoid the need for a dedicated qualification life test unit in the design verification test program, should be limited to 10 operational cycles or less.

4.2.3.10 **Motor verification** - Motor performance testing **shall** be conducted using flight-representative drive electronics.

Note: *The minimum risk flight program will ensure that the design of the flight drive electronics is completed prior to qualification testing of the motors, and flight-representative test electronics are utilized exclusively for qualification and flight acceptance testing all motor types.*

4.2.3.10.1 **Stepper Motors** - Formal qualification/protoflight testing, and/or flight acceptance testing, of the flight stepper motor **shall** be conducted with a physical representation of the driven load (inertia and drag torque) powered by flight-representative drive electronics driven at the expected pulse-rate for flight usage.

Rationale: The performance of stepper motors is highly dependent on the input electrical drive pulse; the inertial loads and the torque drag loads. It can be extremely difficult to assess even minor differences in any of these parameters without conducting actual verification testing under environmental conditions.

4.2.3.10.2 **Electronically-commutated DC brushless motors** - Formal qualification/protoflight tests and flight acceptance testing of the flight electronically-commutated brushless motor **shall** include characterization of torque holes at the commutation switching points, while powered by flight-representative drive electronics, and at a slow enough rotational speed that prevents inertial effects from masking the presence of a torque hole.

Rationale: Electronically-commutated motors must be demonstrated by test to operate compatibly with the commutation electronics and motor rotor position sensors, precluding exhibition of excessively low or zero torque rotor positions.

4.2.3.11 **Mechanism design for maximum output torque/force** - The entire drive train of a mechanism design **shall** be capable of sustaining the maximum output torque or force of the driving actuator under maximum input voltage and worst-case temperature conditions, as well as the combination of maximum actuator output torque and transient dynamic loading from mechanical stop impact at the maximum worst-case velocity of impact.

Note: *This DP applies when operating with the defined motor electrical interface from the motor controller, e.g., with motor input current-limiting protective measures functioning as specified. It is also strongly encouraged to ensure motor input current-limiting features are in place during all ground testing when using electrical support equipment, to prevent flight hardware damage due to human error. (See related Flight Project Practices paragraph 7.2.6 on fault propagation from non-flight equipment.)*

Rationale: The mechanism will experience maximum motor torque if locked-rotor motor stall is encountered in test or flight. It should be capable of surviving the maximum torque/force exposure, including worst-case transient loading from mechanical stop impact at maximum velocity.

4.2.3.12 **Design temperature range for spacecraft mechanisms** - Spacecraft mechanisms **shall** be designed for Allowable Flight Temperature (AFT) limits extended by -15°C and +20°C, or for the wider temperature range that results from the effects of motor or actuator self-heating during functional operation. Furthermore, the upper design temperature bound for spacecraft mechanisms that are operated under ambient conditions **shall** be +35°C, or the higher temperature that may result from the effects of motor or actuator self-heating during ground testing, whichever is more severe.

Note: *Ensure that the junction temperature limits for any silicon electronic devices that may be embedded within an electromechanical actuator comply with Section 4.12.6.*

4.2.4 Mass Properties

4.2.4.1 ***Deleted***

4.2.4.2 ***Deleted***

4.2.4.3 **Control of mass properties** - Methods of positive mass property control (e.g., propulsion latch valves, trim orifices, cover latches, retention of deployables) **shall** be incorporated into the design to preclude unacceptable fluid migration or mass property change.

4.2.5 Structural Design

4.2.5.1 **Structural design requirements** - Flight system structure **shall** meet the design and test requirements of NASA-STD-5001 “Structural Design and Test Factors of Safety for Spacecraft Hardware” (or alternate

standard, e.g., AIAA S-110-2005, for Type 0), and the requirements below.

4.2.5.2 **SC Lift Points & Ground Handling Limit Load** - Hoisting provisions (attachment points and load paths) in flight hardware **shall** be verified to have a non-negative margin of safety for the Ground Handling Limit Load (GHLL), with a safety factor of 1.40 to yield and 1.90 to ultimate strength for structure that is proof-tested (using a test factor of at least 1.20). If metallic flight structure is not proof-tested, then the design factor of safety for the hoisting attachment points and load paths **shall** be 1.9 to yield and 2.5 to ultimate strength. Mechanical Ground Support Equipment (GSE) interfaces to flight hardware, that is not specifically used for hoisting, can be analyzed to the standard design factors of safety per NASA-STD-5001 (or alternate standard, e.g., AIAA S-110-2005, for Type 0).

Note: *The GHLL is a design load, defined as the static weight supported by the ground handling structure times the ground handling dynamic factor Fd. The ground handling dynamic factor, Fd, in the vertical direction is equal to 2.0 unless there is reason to believe that a different dynamic factor is required. Dynamic factors for hoisting flight hardware can be based on actual crane tests with representative loads, but in no instance less than 1.25 is used. The ground handling dynamic factor in the lateral directions is equal to 0.25 unless there is reason to believe that a different dynamic factor is required.*

Rationale: *To ensure design robustness and safety for critical hoisting of flight hardware, the design factors for hoisting attachment points and load paths are increased over the standard factors of safety.*

4.2.5.3 **Joint slip factor of safety** - The minimum factor of safety (yield or ultimate basis) for all spacecraft structure for non detrimental instances of joint slippage, bolt preload exceedance (joint gapping), or bolt contact or encroachment **shall** be 1.00. The minimum factor of safety for detrimental instances (e.g., critical instrument alignment, etc.) **shall** be 1.25.

Note: *The required factor of safety is lower for joints that have room to slip in a benign way because the structure will not be strained, and the alignment isn't critical to performance.*

Verification: *Analysis to demonstrate that preloaded friction joints will not slip or gap.*

4.2.5.4 **Composite fittings factor of safety** - An additional factor of safety of 1.15 **shall** be applied for composite joints, bonds and fittings.

Note: *This additional fitting factor of safety can be reduced to 1.00 if a comprehensive development test program has been performed for the specific joint configuration, tested under representative worst-case loading and environmental conditions.*

4.2.5.5 **Thermally-induced loading factor of safety** - Thermal stresses which occur simultaneously with acceleration or applied forces **shall** be combined in a consistent manner using appropriate yield and ultimate factors of safety. Analysis **shall** verify that the yield and ultimate margins of safety are positive across the qualification/protoflight temperature range for all combined mechanical and thermal stresses.

Positive margins **shall** be demonstrated for metallic structure with the application of a yield factor of safety of 1.00, and an ultimate factor of safety of 1.17, for thermally-induced loading over the qualification/protoflight temperature range. Positive margin **shall** be demonstrated over the allowable flight temperature range using the normal design factors of safety of 1.25 to yield and 1.40 to ultimate. The stress contribution from the acceleration or applied forces **shall** apply the normal safety factors of 1.25 to yield and 1.40 to ultimate for structure verified by testing.

Positive margins **shall** be demonstrated for composite structure, and composite/metallic hybrid structure bond joints, with the application of an ultimate factor of safety of 1.17 over qualification/protoflight temperature range, and an ultimate factor of safety of 1.50 over the allowable flight temperature range. Both of the above cases must be investigated to determine worst-case thermally-induced loading. The stress contribution from the acceleration or applied forces **shall** apply the normal safety factor of 1.50 to ultimate for composite structure.

4.2.5.6 **Structure design criteria for actuators** - Flight system structure **shall** be designed to sustain the maximum output torque or force of mechanism's motors, actuators or preloaded spring elements, with the appropriate design factors of safety from NASA-STD-5001 (or alternate standard, e.g., AIAA S-110-2005, for Type 0), applied to this maximum level. Structural components **shall** maintain a positive margin of safety with the appropriate factors of safety applied when subjected to worst-case transient loads from mechanical stop impact at maximum velocity, or parachute (or other) snatch loads.

Note: *If, when designing the structure, the mechanism maximum output torque or force is not known, then the maximum should be*

assumed to be 2X the nominal output value; and when the mechanism maximum output is known, the acceptability of the structure design will be assessed/validated.

4.2.5.7 **Design temperature range for spacecraft structure** - Spacecraft structure **shall** be designed for AFT limits extended by -15°C and +20°C. The appropriate design factors of safety **shall** apply over this qualification/protoflight temperature range.

4.2.5.8 **Minimum design and test factors for glass and ceramics** – The minimum design and test factors for flight system glass, ceramics, and associated bonds **shall** meet the requirements of NASA-STD-5001B (or alternate standard, e.g., AIAA S-110-2005, for Type 0), with the following exceptions:

a. The ultimate design factor of safety for the usage of non-pressurized glass and ceramics in the flight system **shall** be 2.0 or larger.

b. While NASA-STD-5001B allows verification by analysis of some glass structures, proof-testing is required for all nonmetallic flight structures at JPL. An approved waiver is necessary if 100% proof-testing is not conducted for flight system glass, ceramics, and associated bonds.

Note: *Proof-testing of non-pressurized glass elements and associated bonds within a flight instrument or structure, to the 1.2 test factor, is typically accomplished during protoflight dynamics testing, which subjects the test article to a factor of 1.4 over the predicted limit load. Only rare cases exist where the applied test factor will fall short of 1.2 times the flight limit load for non-pressurized glass elements, if tested to the protoflight level. Flight acceptance test levels may not be appropriate for flight hardware containing glass elements.*

Rationale: This Design Principle reduces the requirements of NASA-STD-5001B for ceramics and non-pressurized glass to the values commonly used for nonmetallics at JPL and has a long successful heritage in instrument piezoelectrics and optical glass elements. Most if not all applications using glass/ceramic elements in flight hardware will be adequately proof-tested by their participation in subsystem dynamics testing at protoflight levels, and thus compliant to this design requirement.

4.2.5.9 **Design validation** - Design verification and validation **shall** be accomplished by a combination of analyses and tests according to the

requirements of JPL Standard Spacecraft System Dynamic and Static Testing. Where testing on a subset of structural elements may not be practical, these primary structural elements **shall** be designed with high safety factors (>2.0 ultimate) to reduce the risks of structural failure. Although structural loads testing is normally required on all primary structure, exceptions for this subset can sometimes be made if the structure is: all metallic ("no test" is not an option for composites), a high safety factor (>2.0) is used in the analysis, and the "no test" criteria enumerated in NASA-STD-5001 "Structural Design and Test Factors of Safety for Spacecraft Hardware" (or alternate standard AIAA S-110-2005, for Type 0) are met.

4.2.5.10 Wire Rope Design and Test Requirements

4.2.5.10.1 **Wire Rope Design** - Wire rope assemblies used in critical flight systems **shall** be designed using the factors of Table 4.2.5-1, with considerations of static preload, maximum launch/landing loading, and dynamic effects such as the functional shock loading in mechanisms when determining the flight limit load.

4.2.5.10.2. **Wire Rope Test** - Wire rope assemblies used in critical flight systems **shall** be pre-stretched and static-proof tested prior to flight usage according to the requirements of Table 4.2.5-1.

Table 4.2.5-1 – Wire Rope Requirements

Wire Rope Application	Example	Minimum Design Factor	Static Proof Test Factor
Statically-loaded	Preloaded launch restraints where wire rope is severed or released	2.0	Pre-stretch wire rope assembly (rope plus end-fittings) to 50% MBS*, or 1.2x Flight Limit Load (FLL), whichever is greater.
Dynamically-loaded, deployments	Wire ropes articulated in one-time deployment mechanisms	2.2	
Dynamically-loaded, with cyclic life	Wire ropes articulated in mechanisms	2.5	
Safety-Critical applications	Wire ropes in flight systems where failure could result in human injury or death	4.0	Pre-stretch rope assembly to 50% MBS*; Proof-test to 2.0x FLL
Nonmetallic rope and cord	Preloaded launch restraints where nonmetallic rope or cord is severed or released	4.0	Proof-test to 1.2x FLL

*MBS = Minimum Breaking Strength

Note: *Design factors of 4.0 and greater are strongly recommended for wire rope applications where numerous articulations over sheaves, and/or bending reversals, are necessary. Bending endurance capabilities of the wire rope must be considered.*

Rationale: These rules follow the general philosophy of existing wire rope standards: pre-stretching where tension stability is necessary, the use of increased safety factors for wire ropes that demand articulation in their operational life, and consideration that wire-rope is functionally a moving mechanical assembly and is subject to degradation from bending and friction effects.

4.3 Power/Pyrotechnics Design

4.3.1 General

4.3.1.1 **Power system grounding/fault tolerance** - The prime power distribution high and return lines **shall** choose either:

a. DC-isolated from spacecraft chassis by at least 2 K ohms and operate within specification both with the power bus balanced about ground (chassis) potential, and when either side (high or low) of the power bus is shorted to chassis.

b. The prime power can be hard referenced to chassis, provided comprehensive protective measures against high side short circuit to chassis exist throughout the system design in all circuitry, cabling, etc. vulnerable to a single fault ending the mission, and such design has successful flight history.

Note: *Typical protective measures include double insulation of all power bus cabling, ample spacing (in circuitry, connectors, printed wiring board traces, etc.) between high side and return or chassis, ample insulation of high power components heat sunk directly to chassis, and routing of power bus cabling away from sharp edges and other sources of insult to the integrity of the cabling insulation. Also see 4.10.2.*

Rationale: To ensure that a single fault short to spacecraft chassis anywhere in the distribution system between the power

source, electronics and the user loads does not pose a catastrophic failure.

4.3.1.2 **Protection for hard grounded power bus applications** - For hard grounded primary power bus implementations, double insulation (or equivalent protection) **shall** be employed in all primary power wiring, solar arrays, and batteries residing upstream of load switches.

Notes:

1. *Double insulation is achieved for the conductor-to-conductor (high side to return) short circuit failure mode via the insulation on each of the two conductors.*

2. *Double insulation is achieved for the high side conductor-to-frame short circuit failure mode via use of a second insulating layer applied to all high side conductors, or cable bundles in which primary power bus high side conductors are routed.*

3. *The "equivalent of double insulation" protection exists when credible single faults do not result in mission-catastrophic failure. Examples are (a) s/c frame is nonmetallic, and (b) there are no credible geometric changes that would cause the s/c chassis to contact the conductor in all areas where only a single layer of insulation is used on the primary power bus high side conductor. Good engineering judgment applies, but the evaluation requires detailed knowledge of the design and good understanding of the system configuration(s) and routing of the primary power bus high side.*

Rationale: Double insulation provides single fault tolerance against the potential mission-catastrophic failure that would result if the primary power bus high side contacted s/c chassis (frame), or a conductor carrying the primary power bus return.

4.3.2 Power Distribution

4.3.2.1 **Load removal** - When a balanced-about-chassis power bus architecture is used, prime power on/off switching of electrical loads **shall** (*should* for Type II) be done by "simultaneously" switching both high and return sides. When a hard-grounded power bus architecture is used, prime power on/off switching may be done by switching only the high side.

Note: *The design should ensure total load removal (i.e., no possible ground return sneak paths) in case of power-related faults. The possibility of a switch "stuck on" failure may require that a second*

series-connected high side switch be used with hard referenced power system architectures.

4.3.2.2 **Bus protection** - Spacecraft primary power bus interfaces **shall** be implemented with in-rush current surge suppression protection and with load removal capability to “clear” a load fault.

4.3.2.3 **Load shedding architecture** - The design **shall** have the capability to establish the state ("on" = critical, and "off" = non-critical) of each s/c load following restoration of power in the event of a primary power bus fault. Hardware assignment (critical or non-critical) **shall** be consistent with time critical mission load requirements and maintaining spacecraft safety and ground commandability.

Rationale: In the event of a power bus fault, non-critical loads can be shed to deliver the available power to the critical loads, and improve the likelihood of recovery.

Note: *Implementation examples are (a) critical and non-critical primary power buses, and (b) a power switch design that has the capability to select the power-on-reset state.*

4.3.3 Power Generation

4.3.3.1 ***Deleted***

4.3.3.2 **Power demands** - The design **shall** supply power to meet, with margins as specified in Section 6.3, the system-wide demand in all mission-critical and mission-enabling modes of operation.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

4.3.3.3 **Primary battery depassivation** - All missions that incorporate primary batteries susceptible to developing a passivation layer **shall:**

a. Include a circuit for battery depassivation. The discharge circuit capable of discharging each battery at the maximum planned discharge rate and discharging a minimum of 3% of battery capacity, or

b. Prove via analysis, and/or test data, that passivation layer accumulation is not an issue for the mission and storage durations planned for the S/C, based on the battery chemistry being used.

Rationale: The purpose is to avoid voltage delay, where the battery output voltage could dip below minimum bus voltage requirements. Voltage delay is caused by a passivation layer being built up on the electrode surfaces during extended storage. Voltage delay may not apply to all battery chemistries.

***Note (Glossary item)**: Passivation Layer: A passivation layer is a resistive residue that accumulates over time on an internal battery electrode (e.g., anode), when a battery is not being used. This layer adds resistance to any external circuit loop supplied by the battery whenever the battery is being used. This resistance decays (is 'burned-off') once the battery circuit is closed. The time required to eliminate this layer is largely a function of the amount of current being used by the external circuit, battery temperature and the history of the battery.*

4.3.3.4 **Recovery from loss of power** - Once power is restored after a complete or partial loss of power, the spacecraft **shall** (*should* for Type II and Type 0) recover baseline functionality, assuming there is no collateral damage (including failure to execute a time-critical event) as a result of the power outage.

Rationale: Power glitches should be survivable. For example, the power system should not be damaged due to the power loss alone, assuming there was no collateral damage due to factors external to the power system.

Rationale: The early Cassini design was not consistent with recovery from loss of power. The risk of transient outages resulting in loss of memory was determined to be an unacceptable risk, and the design was changed to accommodate the outages.

4.3.3.5 **Energy storage** - Power system designs based on solar power **shall** include energy storage, with margins as specified in Section 6.3, to supply power for peak loads and to deliver power during off-sun mission events, e.g., launch, eclipses, Trajectory Correction Maneuvers (TCMs), day-night cycles, and credible anomalies.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

***Note:** Energy storage for short-term, large peak step loads, e.g., propulsion valve actuation, may be more efficiently accommodated using a capacitor bank, thereby allowing a smaller battery on solar powered missions.*

Note: *Stored energy after acceptable Depth-of-Discharge (DOD) (as discussed below) is not considered power or energy margin. For power or energy design margin, follow the requirements set out in Section 6.3.*

Note: *The battery charging algorithm should accommodate the predicted roll of the spacecraft, where the solar arrays are periodically exposed to the sun, with adequate margin to accommodate 3-sigma roll anomalies.*

4.3.3.6 **Secondary (rechargeable) batteries** - When energy storage is implemented via a secondary battery (rechargeable), the sizing is based on the following.

4.3.3.6.1 **Mission phase depth of discharge** - Secondary batteries **shall** be sized to have acceptable DOD's in all mission phases.

a. The following definition of DOD is used for batteries:

   DOD = 100% * (battery capacity removed during discharge [Ah]/battery capacity total [Ah])

b. Battery capacity removed during discharge (e.g., Amp hours) **shall** be based on the CBE (Current Best Estimate) plus uncertainty of loads with the worst case profile for the particular mission phase being evaluated, e.g., worst case launch day within launch period

c. Battery capacity **shall** be based on the worst-case capacity for the mission phase and scenario being analyzed. This needs to account for the worst combination of temperature, discharge rate, and battery calendar, and cycle life to be encountered during the mission. This means that the battery capacity may be a function of conditions that change with mission phase.

Rationale: *The DOD limit is intended to provide adequate lifetime for most missions considering battery aging, battery performance uncertainties, and load uncertainties.*

4.3.3.6.2 **Single fault tolerance** - Secondary batteries **shall** (**not** required for Type II, *should* for Type 0) be implemented to survive a single failure including an open-circuit cell, or a short-circuit cell, and operate within the DOD limits specified herein after sustaining such failure.

Note: *The single failure tolerance requirement can be met by multiple battery strings, or extra cells in a single string with bypass circuits (diode(s) or electro-mechanical) around each one.*

Note: *The launch case is also subject to the single failure tolerant requirement, even though battery single failure scenarios relevant to launch are unlikely, that is a failure occurring during launch is unlikely given the short window of vulnerability, and even though it is unlikely launch would proceed were a battery single failure known ahead of time.*

4.3.3.6.3 **DOD limits for cyclic operations** - For cyclic operations that use battery energy at intervals, the maximum DOD, which depends on the number of battery cycles, **shall** (*should* for Type II and Type 0) be in accord with Table 4.3.3.6-1, applicable to both NiH2 and Li-Ion battery types.

Table 4.3.3.6-1 DOD limits for cyclic operations

Number of cycles	Allowable DOD
<100	<70%
100 < # cycles < 5,000	<60%
5,000 < # cycles < 30,0000	<40%
> 30,0000	<20%

Note: *A battery cycle is defined as any time the battery is discharged to 50% or more of the allowable DOD and recharged to near full.*

Note: *Battery chemistry may affect the acceptable DOD.*

Note: *Mission class may affect acceptable DOD.*

4.3.3.6.4 **DOD limits for single or occasional use** - The acceptable design DOD for single, occasional, or unplanned occurrences, such as launch or safe-hold, **shall** (*should* for Type II and Type 0) be a maximum of 70% at worst case conditions assuming typical aerospace quality NiH2 and Li-Ion batteries are used.

Note: *Accommodates worst-case durations for launch, eclipse, tumbling, etc. conditions.*

Rationale: *A limited DOD allows for uncertainties in the knowledge of the actual battery energy available. Also, deeper discharges may limit battery life later in the mission. It is prudent to maintain the battery at a safe DOD by design.*

4.3.3.7 **Primary (non-rechargeable) batteries** - Primary batteries (non-rechargeable) **shall** operate at less than 80% DOD after one failure. The capacity used for DOD calculations must account for de-rating for temperature, discharge rate, and lifetime effects. The design DOD **shall** include all battery discharge events including for example pre- and post launch testing and depassivation in addition to the energy used during the functional life.

Note: *DOD is defined as in 4.3.3.6.1 (a, b, and c).*

Rationale: *The 80% DOD requirement on the battery covers uncertainty in the energy produced by the battery and the de-rating factors applied.*

4.3.3.8 **Thermal batteries** - Thermal batteries **shall** (*should* for Type II and Type 0) operate at less than 80% DOD under worst case operating conditions, and **shall** (*should* for Type II and Type 0) have a 30% margin against active lifetime, and 30% margin against discharge rate capability. Fully redundant thermal batteries **shall** (**not** required for Type II or Type 0) be used for all critical functions.

Note: *Pyrotechnic initiation is a common critical function for which separate thermal batteries are used to power the independent strings (i.e., "A" and "B" sides) for redundancy.*

Rationale: *Thermal batteries are different than the other types of batteries. In addition to DOD, they need to be designed for the length of operating time and discharge rate(s).*

Note: *DOD is defined using the available capacity based on the manufacturer's specification.*

Note: *DOD may not be the limiting factor in sizing the battery. Peak discharge rate required to fire pyros is often the dominant sizing parameter.*

4.3.4 **Pyrotechnic Function**

4.3.4.1 **Simultaneous firings**

a. The design **shall** have the capability to guarantee- under worst-case conditions (temperature, voltage, etc.) - simultaneous firing of pyro actuation device(s) as is required by the specific system design- noting number of devices and simultaneity.

b. The design **shall** (**not** required for Type II or Type 0) have the capability to guarantee firing up to 6 NASA Standard Initiators (NSIs) simultaneously when mechanical separations are planned, under worst-case conditions (temperature, voltage, etc.).

Rationale: To ensure successful activation, and mechanical separation where multiple devices are used, such as heatshield separation or stage separation.

Note: *In the case of the NSI, there are two NSIs in each pyro-actuated device and/or mechanism, and each NSI is initiated individually from a redundant firing string. It is common to require 3 simultaneously pyro-actuated devices (that is 6 NSIs total) firing for stage, heatshield, backshell, etc. separations.*

Application Note: *"Simultaneous" A- and B-side activation of initiators may be intentionally staggered somewhat (i.e., separated in time) to account for device-specific operating parameters. The power delivery should be capable of simultaneous delivery of the necessary current to both strings, or capable of separating the timing as necessary.*

Note: *See also section 4.10.4.4.*

4.3.4.2 **Current limiting** - Pyro circuits **shall** incorporate current limiting to control maximum circuit current flow.

a. Current limiting **shall** (**not** required for Type II) accommodate the full pulse width of the activation period.

b. Sizing of electronics components **shall** ensure piece parts meet the derating guidelines of JPL Derating Standard, or an alternate, approved, derating document for Type 0, both under nominal (worst-case) conditions and anomalous (worse-case) conditions of a pyro high-side short to chassis.

Type 0 projects **shall** document which derating document they will use in their approved Project Plan if not the JPL Derating Standard.

c. Cabling, printed wiring board circuit traces, connector contacts, and all other elements in pyro circuits **shall** demonstrate positive margin and no degradation under worst-case conditions, including repeated firings into a NSI high-side short to chassis for those affected elements.

Rationale: (1) Required to limit unwarranted current flow from low impedance source (e.g., battery), and thus protect against damaging stress. It will also ensure (2) circuit operation and component stress levels consistent with analysis, (3) ensure safe/survivable operation in case of an activation device short to return, and (4) ensure safe and survivable operation during ground testing.

Note: *The components and design should be sized to demonstrate margin against the mission planned use after live pyro firings that are part of the system test program including any need for retest, e.g., handle a minimum of 4 operational cycles at full current and duration (2 test, 1 flight, 1 margin).*

Note: *Typical firing current for a NSI should be limited to 5-7 A.*

4.3.4.3 **Enabling of pyrotechnic functions** - The s/c design **shall** provide an enable function for each pyro event. Pyro functions can be enabled in groups when mission success is not dependent on the firing order or sequence of the pyro functions within each enabled group.

Rationale: Separate and independently commanded 'enable' and 'fire' functions, implemented in series fashion, provide protection against single failures, e.g., in the 'fire' circuitry, inadvertently energizing a pyrotechnic. When the order in which the pyros are fired makes no difference to mission success, then they may be simultaneously enabled as a group- because failure of a 'fire' circuit has no adverse impact. When the order of pyro events is essential for mission success, then these events must be enabled separately from each other- to be tolerant of potential single failures in the 'fire' circuits. Single failure of a 'fire' or 'enable' function to activate the pyrotechnic is overcome by using redundant A- and B-side pyro circuits.

Note: *The timing by when pyro functions are enabled should take into consideration the possibility that with a failed 'fire' circuit, a pyro event could occur when the 'enable' is given.*

Note: *Unintended activation of pyrotechnics is prevented by a series of four independent functions: Inhibit, Arm, Enable, and Fire. The Inhibit function is used in ground operations including at the launch pad. The Inhibit is typically removed by launch vehicle separation or other action at launch. The Arm function is activated at the launch pad. The Enable function is activated shortly before actual activation of the pyro. The Enable often affects groups of pyro functions. The Fire function is the last required action that sends electrical current to activate a specific function or NSI.*

4.3.4.4 **Duration limiting** - The design of the firing circuits **shall** limit the duration of pyro current flow.

Rationale: NSI activation can result in a near zero resistive path to case at the device in which the NSI is installed with attendant high current flowing in pyro circuits until shut-off.

Note: *The duration of activation of the fire circuit must consider both the maximum time needed to fire the initiator plus the time needed to activate the circuit. Relays may take several milliseconds to transfer; Field Effect Transistor (FET) switches may be much faster. Typical durations for the firing circuit are 10 to 20 ms.*

4.3.4.5 **Pyro bus return** - Pyro bus return **shall** be isolated from s/c chassis.

Note: *This requirement must be met even if the pyro bus is on a separate power source, e.g., thermal battery.*

Rationale: To prevent chassis current (during nominal activation and/or pyro failures), which might interfere with other s/c subsystems.

4.4 Information System Design

4.4.1 General

4.4.1.1 Redundant handling of critical data

a. For data critical to the mission (e.g., launch, flyby science, orbit insertion, EDL, etc.), the design **shall** provide the capability for onboard storage of that data.

b. For data critical to the mission (e.g., launch, flyby science, orbit insertion, EDL, etc.), the design **shall** (*should* for Type II and Type 0) provide the capability for simultaneous real-time transmission of that data.

Note: *Also see 3.1.3 and 7.1.2.*

4.4.2 On-board Processing

4.4.2.1 **Utilization of limited tracking coverage** - The system design uses data editing, data compression and improved data encoding techniques to meet downlink telemetry data requirements and to limit demands on tracking by the Deep Space Network (DSN). This reflects the fact that DSN aperture time is a limited resource.

4.4.2.2 **Identification of s/c data** - Data transmitted to the ground **shall** be identified so the ground can track it, report its status, request retransmission, and route it upon receipt.

Rationale: Raw data without appropriate contextual or temporal identifiers creates operability issues. The identification of spacecraft data enables data accountability between the various system elements across the end-to-end information system.

4.4.3 On-Board Storage

4.4.3.1 **Protection of critical data** - Stored critical data **shall** be protected from loss, e.g., due to credible fault scenarios.

Note: *Data criticality is project-specific.*

4.4.3.2 **Compatibility with tracking outages** - The information system design **shall** have bulk data storage capability to enable storage of time critical science data and/or engineering telemetry data during long non-track periods and accommodate flight operational uncertainties caused by weather effects or ground tracking station problems.

4.4.3.3 **Data storage** - The design of on-board data storage **shall** accommodate overall communications system performance needs, including requirements for return data volume, latency, priority, and quality.

4.4.3.4 **Protection from Single Event Upsets (SEUs)** - The design **shall** protect on-board stored data susceptible to upset, e.g., from SEEs.

Note: *For example, by storing multiple copies, use of Error Detection And Correction (EDAC), etc.*

4.4.4 Commanding and Sequencing

4.4.4.1 **Use of toggle and step commands** - Toggle commands and step commands **shall** be permitted only if absolute position commands and telemetry also exist for the same function(s).

Rationale: To avoid needing to predict the s/c state that will exist at the time of command execution.

4.4.4.2 **Multi-function commands** - Any command controlling two (2) or more independent functions **shall** include a “no change” option as a valid parameter for control of each function.

Note: *Avoids needing to know the current state of each parameter and re-asserting it in each command.*

4.4.4.3 ***Deleted***

4.4.4.4 **Assured commanding** - The design of information system commanding functions **shall** be implemented in a manner robust to power outages and degraded communications capabilities, e.g., hardware command decoding, non-volatile memory.

Note: *This includes command reception, decoding, routing, storage, sequencing, distribution, and execution.*

4.4.4.5 **Commanding modes**

The s/c **shall** provide capabilities for real time commanding and stored sequence commanding, where stored sequence commanding is the primary commanding mode of operation.

4.4.4.6 **Commanding reliability**

The s/c **shall** provide:

a. Protection against all incorrect commands.
b. Protection against correct but untimely commands that:
    i. risk s/c health or safety,
    ii. initiate irreversible s/c state changes,
    iii. have the potential to deplete s/c consumables to an extent that threatens the planned mission, or

iv. jeopardize s/c commandability.

Note: *Also see 4.1.3.2, 4.11.4.2*

4.4.4.7 **Commanding in the blind** - The s/c **shall** support an uplink-commanding mode of operation that does not rely on 2-way communications.

Rationale: To respond to s/c emergencies, e.g., off-pointing from Earth

4.4.4.8 **Onboard command processing approach** - Direct memory location or content manipulation **shall** be avoided for onboard command processing. Instead, use software functions to translate commands into the appropriate actions. This includes commands that change parameters.

Rationale: Addresses Mars Global Surveyor mission-ending commanding error. Direct modification or manipulation of memory contents, especially as the nominal method for operating a spacecraft, introduces unnecessary risk of inadvertent and incorrect modification of memory contents.

Note: *Current practice dictates that the flight software should be implemented such that there is an onboard translation of commands into software functions so that no direct knowledge of memory locations is necessary. In addition, this principle does not prohibit the inclusion of commands to manipulate memory directly for diagnostic or contingency purposes.*

4.4.4.9 **Two independent commands or actions for hazardous ground or mission critical events** - The initiation of hazardous ground or mission critical in-flight events **shall** require at least two independent commands or actions.

Rationale: Multiple independent actions help to reduce the possibility that hazardous or mission critical actions will occur in error or be started prematurely.

Note: *It is important to properly enable non-reversible in-flight or hazardous activities. This principle doesn't require every in-flight action to have two independent commands or actions – only those activities that impart irreversible consequences. An example would be initiating the entry, descent, and landing behavior of the flight software while still in transit to Mars. The implementation can be satisfied by generally applied practices such as requiring an enable command immediately prior to any*

command that is normally prohibited in the current spacecraft mode.

4.4.5 Telemetry Modes and Formats

4.4.5.1 ***Deleted***

4.4.5.2 ***Deleted***

4.4.5.3 **Emergency engineering data mode(s)** - The information system design **shall** have at least one engineering emergency data delivery mode and format for diagnostic use. A hierarchical approach **shall** be used so that assessment of spacecraft health/safety can be rapidly attained.

Note: *This will provide special telemetry to enable operations to diagnose spacecraft emergencies.*

4.4.6 Telemetry Visibility

4.4.6.1 **Visibility of s/c status** - The information system design **shall** (*should* for Type II and Type 0) provide telemetry data to assess spacecraft status under normal, stressed, and faulted operations. This includes health, anomaly determination, and visibility into spacecraft state and any mission unique functions.

Note 1: *The ability to rapidly discern from telemetry the s/c state could enable recovery efforts for a faulted condition in which the s/c only infrequently and momentarily is in view of a tracking station, and thus there is limited ability to gather telemetry data to provide any insight into the s/c condition.*

Note 2: *Designing an information system that meets this requirement is an especially cross-cutting system engineering activity that needs to be undertaken with forethought and care. A well-designed information system provides sufficient visibility during routine operations as well as during and after anomalies, and provides critical diagnostic data during critical operations in case of catastrophic failure. The availability and quality of in-flight telemetry and the downlink bandwidth often present limitations relative to the demand, requiring configurable sampling rates and frame contents, capabilities for prioritization, and preemption.*

Pay special attention to these areas where escapes can occur:

- *Sometimes the necessary telemetry to diagnose a failure is not physically available because it was not implemented in the electronics. Ensure that all potential SPFs have the necessary telemetry measurements implemented in hardware/firmware so that they are available to the information system.*
- *To the extent possible, ensure that diagnostic telemetry is available in the presence of the postulated fault (in contrast, SMAP secondary power converter voltage telemetry was not available when the power converter voltage was not present, hampering efforts to diagnose the failure).*
- *For providing confirmation of critical activities such as deployments and thruster firings, if relying on indirect telemetry for deployment verification (e.g., IMU data), ensure that the sensors are in fact able to provide the needed data (e.g., IMUs are oriented in axes that are sensitive to the disturbance to be measured, have the necessary sensitivity, and can be sampled at a high enough rate to capture the dynamic signature). For monitoring for potential thruster overheating, ensure the temperature sensors are placed appropriately and have the necessary range.*
- *Ensure the preservation of "breadcrumb" data leading up to a fault such as a reboot or side swap. Often, this is implemented by small circular buffers (e.g., a digital storage unit that can capture high-rate data for a short period for downlink and assessment at a later time).*
- *Ensure that critical telemetry can always get into the downlink and will not be blocked by routine telemetry, both for planned activities and faulted conditions that require urgent ground intervention.*

4.4.6.2 ***Deleted***

4.4.6.3 ***Deleted***

4.4.6.4 **Visibility of spacecraft state** - The telemetry system end-to-end design **shall** permit ground operators, during the first part of a ground tracking pass, to determine rapidly and unambiguously the state of the spacecraft, particularly to determine if the spacecraft executed a fault protection response.

Note: *This enables ground operators to respond rapidly and correctly to spacecraft states with sequences that are consistent with the state.*

4.4.6.5 **Critical sequence telemetry monitoring** - See 7.1.2

4.4.6.6 **POR state visibility** - See 4.12.7.2

4.4.6.7 **Visibility into fault protection state** - See 4.9.3.2

4.4.6.8 **Visibility to reconstruct faults** - Visibility **shall** be provided that would support post-mortem analysis of s/c activities with the potential for mission catastrophic outcome.

Note: *Activities with potential catastrophic outcome include (a) certain mission-critical sequences (e.g., launch, orbit insertion, entry-descent-landing), (b) s/c hazardous operations (e.g., activation and use of the propulsion system), and (c) interaction with uncertain and unforgiving mission environments (e.g., comet or asteroid rendezvous, aerobraking).*

Note: *For Type II missions, this visibility requirement may be satisfied by recording telemetry. For Type I missions, this visibility must also be available via real-time telemetry.*

4.4.6.9 **Visibility during ground test** - Whenever the s/c is powered during ground testing, visibility into s/c operation **shall** be available.

Rationale: Ensures s/c transient behavior (including power-on transients)- if it occurs- will be visible to the test team.

4.4.6.10 ***Deleted***

4.4.6.11 **Data accountability** - The s/c **shall** provide visibility into the receipt and transmission of all data to and from the s/c, and accountings of all data products it handles including status information on data routed and stored, and deletions made.

Note: *This allows ground operators to track the operations of the s/c, and status the products in relation to the uplinked commands. S/C reporting should not depend on receipt of 100% of the reports, rather allow for infrequent outages.*

4.4.7 Timing and Synchronization

4.4.7.1 **S/C clocks & counters** - Spacecraft **shall** continue to operate in the event of rollover of spacecraft clocks and/or incremental counters (hardware or software).

4.4.7.2 **S/C clock drift** - The s/c clock **shall** be included periodically in the telemetry stream.

Rationale: Allows knowledge of the drift between the s/c and ground clocks.

4.4.7.3 **Instrument observation timing** - The flight system **shall** provide a means for the ground to uniquely determine the timing associated with the sampling of each instrument observation.

4.4.7.4 **Engineering telemetry measurement timing** - The flight system **shall** provide a means for the ground to uniquely determine the timing associated with the sampling of each engineering measurement, and the relationship between the engineering measurements and the instrument observations.

4.5 Telecommunications System Design

4.5.1 General

4.5.1.1 **Link default threshold error rate** - The information system and telecommunication system design **shall** achieve an end-to-end uplink and downlink data quality that ensures a low probability of command errors at the spacecraft and a high probability of readable telemetry on the ground. The thresholds for direct communications between a tracking station on Earth and a spacecraft are:

- for uplink command, a Frame Error Rate (FER) < 1e-3, and an Undetected Frame Error Rate (UFER) < 1e-9
- for downlink telemetry, FER < 1e-4.

Note 1: *These specific FER requirements do not apply to proximity links with acknowledgements or to links with the Tracking Data Relay Satellite (TDRS). Proximity links and TDRS links each have their own link threshold definitions.*

Note 2: *A frame refers to a layer 2 data unit (OSI reference model) that a link protocol receives, processes, and transmits. For example, when CCSDS compliant signaling is used, a frame refers to a "TM Space Data Link Protocol" as described in TM Space Data Link Protocol," CCSDS Blue Book, Issue 3, Section 2.1.1, October 2021 - https://public.ccsds.org/Pubs/132x0b3.pdf.*

4.5.1.2 ***Deleted***

4.5.1.3 **Simultaneous command and telemetry** - The design **shall** permit simultaneous command and telemetry capability.

Rationale: This enables command and telemetry handling in the same view period.

Note: *This principle can be met using a single antenna to support both command and telemetry functions, or separate antennas for command and telemetry functions provided the separate antennas provide similar coverage.*

4.5.1.4 **Telecommunications capability for special activities/events** - Telemetry, command, and (where needed) radiometric data capability **shall** (*should* for Type II and Type 0) be available throughout the mission in normal cruise pointing attitude, and during in-flight activities defined by the project as special activities/events, such as all first uses of s/c functionality and all irreversible events.

Rationale: Provides real-time monitoring during cruise and mission-defined special activities, and timely contingency commanding in the event that unexpected behavior is observed.

Note: *When switching of spacecraft components is required to provide the telecommunications capability for the mission-defined special activity, there is a risk trade between the benefit of having the visibility and the risks associated with the switching.*

4.5.2 Command Links

4.5.2.1 **Spacecraft uplink RF carrier** - The spacecraft uplink **shall** use only an ITU (International Telecommunication Union) approved or SFCG (Space Frequency Coordination Group) recommended frequency bands.

Note: *New projects will not be allowed to use S-band for deep space uplinks.*

Note: *This requirement does not apply to optical telecommunications links.*

Note: *For the purposes of this rule, "deep space" is defined as further than 2e6 km from Earth.*

4.5.3 **Telemetry Links**

4.5.3.1 **Spacecraft downlink RF carrier** - The spacecraft downlink **shall** only use an ITU approved or SFGC recommended frequency bands.

Note: *For deep space missions, S-band downlink should be used only for radio science, radiometrics, and critical communications, and then only the lower half of the S-band frequency allocation should be used, in order to avoid conflicts with the spectrum allocated for mobile phone use.*

Note: *This requirement does not apply to optical telecommunications links.*

Note: *For the purposes of this rule, "deep space" is defined as further than 2e6 km from Earth.*

4.5.3.2 ***Deleted***

4.5.4 **Relay Links**

4.5.4.1 **Accommodation of fades** - Surface-to-orbit links, or surface-to-surface links **shall** be able to accommodate greater than or equal to 10 db fades.

Rationale: Relay links are characterized by considerable geometric variation as well as possible multi-path effects from landed or orbiter vehicle structural reflections or surface (ground) reflections.

4.5.4.2 **Relay link performance measurement** - The performance of relay links **shall** be measured, and the results included in the s/c engineering telemetry.

Note: *Measurements support flight operations decision-making regarding use of the relay link.*

4.5.5 **Telecommunication System Margins**

4.5.5.1 **Design to requirements** - Telecommunication equipment, antennas, and ancillary hardware ***should*** be the minimum needed to meet the mission and system telecom requirements with acceptable risk and operating margin.

4.6 Guidance, Navigation & Control Design

4.6.1 General

4.6.1.1 **Architecture** - Feedback control is used where driven by considerations of stability and performance to reduce uncertainty and disturbance-induced errors. Feed-forward control is used where needed by performance or diagnostic considerations (e.g., to reduce transient response times, and enable health diagnosis approaches based on monitoring the control error magnitude).

4.6.1.2 **Minimum gain and phase margins** - Minimum gain and phase margins in control systems **shall** be as follows.

a. for high performance control designs: 6 db, 30 degrees

b. for robust control designs: 10 db, 60 degrees

Note: *Gain and phase margins are defined using full "keep-out" regions in the vicinity of the Nyquist critical point.*

Rationale: Ensures stability and robustness in the presence of uncertainties

4.6.1.3 **Gain-stabilized resonance modes** - Frequencies of gain-stabilized resonance modes **shall** reside sufficiently above the control bandwidth so as to not interfere with the control system function.

Note: *Ideally, at least one order of magnitude exists between the control bandwidth and the lowest resonance frequency.*

4.6.1.4 **Sampled control system timing** - Sampling rates used in control systems **shall** be chosen much larger than the control bandwidth and with considerations for system delays.

Note: *A general rule of thumb for sampling frequency is expressed as follows:*

Sampling frequency > {[10 + (20)(number of full sample delays)] * control bandwidth}

Rationale: Ensures appropriate level of robustness and stability margins

4.7 Propulsion System Design

4.7.1 General

4.7.1.1 **Design and test requirements** - Propulsion elements and other pressurized components **shall** meet the design and test requirements of ANSI/AIAA S-080 “Space Systems - Metallic Pressure Vessels, Pressurized Structures and Pressure Components” and ANSI/AIAA S-081 “Space Systems - Composite Overwrapped Pressure Vessels (COPVs).”

Rationale: Both of these ANSI/AIAA specifications have been adopted by NASA for human and robotic space programs, and are the industry standard for design and testing of propulsion systems.

Note: *Use latest revision, no earlier than Rev A-2018 for S-080 and Rev B-2018 for S-081.*

4.7.1.2 **Demonstration of operating point** - Safe, reliable operation of propulsion subsystem components (e.g., valves, thrusters) **shall** be demonstrated by tests over a range of conditions that envelope flight operations expectations, including appropriate margins to cover uncertainties (e.g., feed pressures, flow rates, mixture ratios, high voltages).

4.7.1.3 **Use of coupled thrusters** - When precise navigation control is required by the mission design, thrusters **shall** be used in a balanced couple configuration.

Rationale: Minimizes the uncertainty in modeling the delta-velocity imparted during maneuvers.

4.7.1.4 **Shielding for debris impacts** - Earth orbiters **shall** provide adequate protection of pressure vessels from impact by orbital debris.

Rationale: For Earth orbiters, impact-induced explosions of pressure vessels present a risk to both the flight system and to other assets in orbit. Hoop stress makes the pressure vessel more vulnerable to rupture, which would possibly generate debris. Shock-induced decomposition of hydrazine propellant could cause catastrophic break-up of the flight system. Leak-before-burst tank designs only apply to static conditions, not to hypervelocity impact by orbital debris. Thermal blankets, even with added beta cloth, typically do not provide sufficient protection against the debris environment in low Earth orbit.

More substantial shielding such as spacecraft structure is needed.

4.7.2 Sizing

4.7.2.1 **Propellant tanks** - Propellant tank volume **shall** be sized to accommodate the nominal mission based on the required deterministic and statistical delta velocity (see Section 3.2.1) needs (based on the total mass allocation), and including consideration of needed ullage.

4.7.2.2 **Propellant** - Propellant load estimates **shall** be based on specification minimum Specific Impulse (I_{sp}) value for engine/thruster and allocated spacecraft system mass.

4.7.3 Propulsion Design Margins

4.7.3.1 **Component cycle life margins** - Propulsion components (e.g., chemical thrusters, catalyst beds, engine coatings, etc.) that function in a cyclic manner **shall** demonstrate a life capability with greater than 50% margin beyond the worst-case planned mission usage.

Verification: based on the hardware heritage, prior mission use or qualification testing with a dedicated test unit.

4.7.3.2 **Rocket engine life margins** - Rocket engines **shall** demonstrate a life capability with greater than 50% margin beyond the worst-case planned mission usage, with respect to propellant throughput, operating time-at-temperature, and deep thermal cycles, as applicable.

Verification: based on the hardware heritage, prior mission use or qualification testing with a dedicated test unit.

4.7.3.3 **Propulsion mechanisms cycle life margins** - Propulsion component mechanisms such as engine gimbals and valves **shall** meet the cycle life design margin requirements of Section 4.2.3.9 herein under worst-case thermal conditions.

4.7.3.4 **Electric thruster life margins**

4.7.3.4.1 **Electric thruster minimum life test** - Electric thrusters **shall** demonstrate by life test a total impulse capability of 100% of the planned worst-case mission usage.

4.7.3.4.2 **Electric thruster impulse margin** - Electric thrusters shall demonstrate by test or analysis, a margin of at least 50% (factor of 1.5 times the required life).

4.7.3.4.3 **Electric thruster cycle margin** - Electric thrusters **shall** demonstrate by test greater than 50% margin beyond the planned worst-case number of deep thermal cycles (factor of 1.5 times the required number of cycles).

4.7.3.5 **Electric thruster voltage margins**

4.7.3.5.1 **Electric thruster voltage margin** - Electric thrusters **shall** demonstrate a high voltage stand-off margin of greater than 50% under worst-case conditions.

Note: *High voltage standoff margin is defined as follows:*

Margin = 100% * {[Minimum breakdown voltage/Maximum operating voltage] -1}

4.7.3.5.2 **Electric thruster voltage margin verification** - Voltage margin verification **shall** be by testing under environmental conditions while not operating but with propellant flow.

4.7.4 Safety

4.7.4.1 ***Deleted***

4.7.4.2 **Use of passive isolation in bi-propellant systems** - Bi-propellant propulsion systems **shall** incorporate a passive means of ensuring that liquid fuel and oxidizer are prevented from mixing in the pressurization system or tanks.

4.7.4.3 **Use of gas regulators** - Gas regulators (single or series redundant) **shall** be avoided to provide isolation of pressurant from the propellant tank. Instead, isolation devices such as latch valves or pyrotechnically actuated valves **shall** be incorporated for long periods of quiescent operation.

Rationale: Experience shows that gas regulators can leak, sometimes at rates far in excess of the device specification.

4.7.5 Propulsion Temperature Test Margins

4.7.5.1 **Qualification without propellant** - Propulsion hardware **shall** be qualified to the typical thermal test margins of AFT -15°C/+20°C when not wetted by propellant or other fluids that would not be liquid at these temperatures.

4.7.5.2 **Qualification with propellant** - When testing with propellants is required, as in rocket engine hot firing qualification tests, the hardware **shall** be qualified for operation at temperatures 10°C below the minimum AFT and 10°C above the maximum AFT.

Rationale: Test margins may be reduced due to the limited liquid temperature range of the propellants, and the known sensitivity of some propulsion hardware to thermal effects.

4.8 System Thermal Design

4.8.1 ***Deleted***

4.8.2 Temperature Control Design Performance

4.8.2.1 **Temperature control design margin** - Thermal control design margin is defined as the difference between the Allowable Flight Temperature (AFT) upper or lower bound, and the worst-case predicted hot or cold bound (respectively). Worst-case predicted temperatures are defined as the combination of realistic (non-anomalous) thermal extremes during the mission that may produce the maximum hot and minimum cold temperature extremes. Figure 4.8.2-1 illustrates the temperature control design margin as well as the relationship among temperature control ranges used in the verification of flight systems.

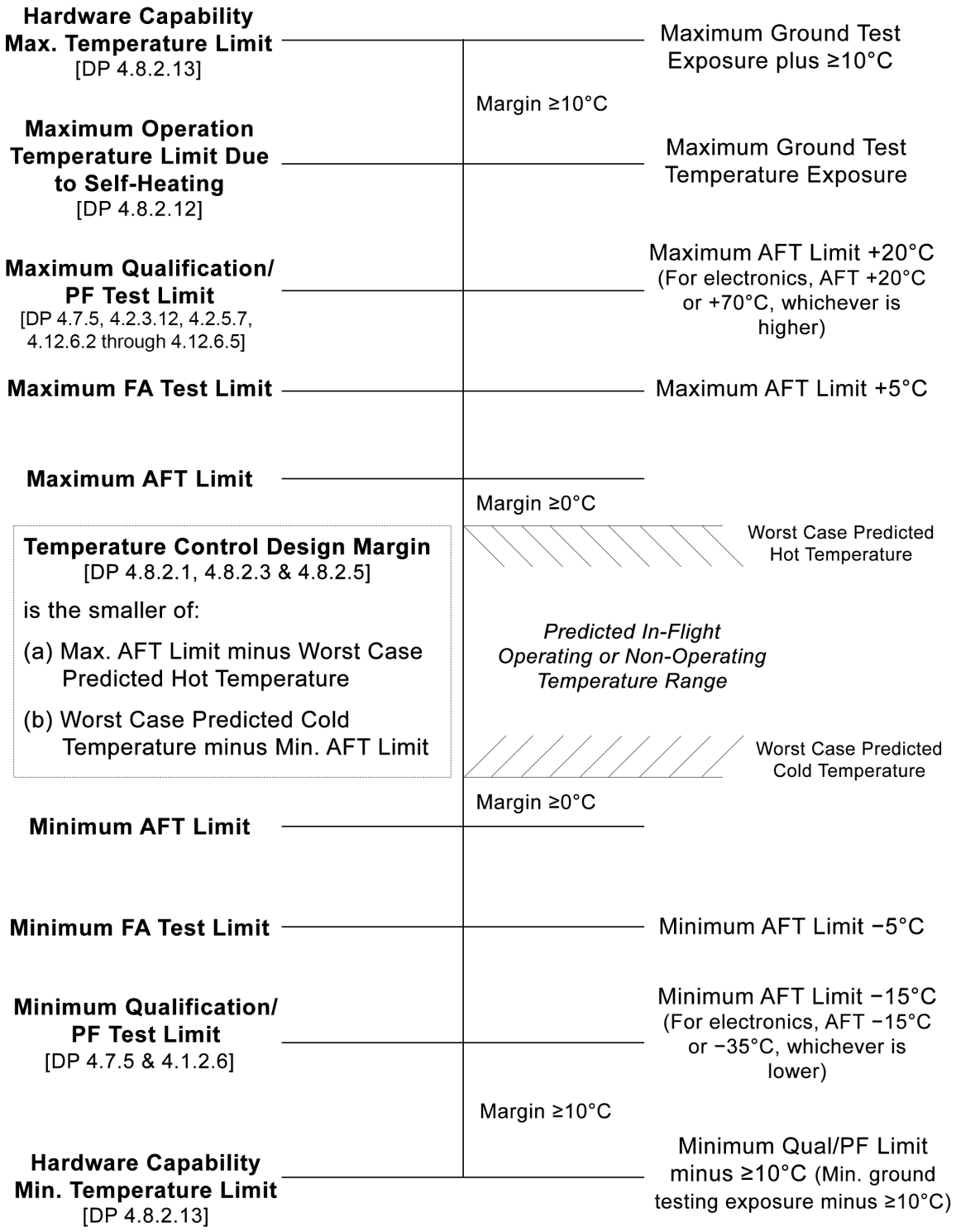

Figure 4.8.2-1 **Temperature Control Limits and Margins**

4.8.2.2 ***Deleted***

4.8.2.3 **Design margin under nominal and worst-case conditions** - The thermal design **shall** control temperatures within the defined Allowable Flight Temperature range (AFT).

Rationale: To ensure no credible thermal threat to hardware when operating under nominal and worst-case operating conditions.

4.8.2.4 **Recoverability of AFT limits** - The AFT limits of any unit designated as critical to mission success **shall** (*should* for Type II and Type 0) be recoverable upon detection and resolution of the single fault and subsequent ground intervention.

Note: *Temperature control of flight system mission-critical functions must be single fault-tolerant, e.g., redundant heaters.*

4.8.2.5 **Design margin under anomalous conditions** - The thermal design **shall** (*should* for Type II and Type 0) control temperatures within the defined Qualification/Protoflight (Qual / PF) temperature range during the mission under credible failure mode conditions that result from s/c potential single failures and ground operator errors.

Note: *Examples of credible abnormal conditions are anomaly-induced power dissipation and/or off nominal sun attitude conditions. Constraints to analyzing abnormal conditions that are necessary to maintain the thermal control with these limits, e.g., duration of unplanned power-off states, duration of time that attitude control can be lost, etc., are identified and resolved via the system engineering process.*

Note: *Transient solar illumination into an instrument aperture or normal to an instrument radiator can result in violation of the detector PF temperature limits and permanent damage. Where appropriate, the project defines the required duration of boresight or radiator solar exposure that must be tolerated during a loss-of-attitude recovery.*

4.8.2.6 **Design margin to propellant freezing** - Hardware **shall** be thermally controlled to remain a minimum of 10°C above the propellant freezing temperature whenever the hardware is in contact with propellant or propellant vapor.

4.8.2.7 **Design margin to propellant condensation** - Pressurization system hardware that will come in contact with propellant vapor **shall** be thermally controlled over the entire mission to remain a minimum of 10°C

above the temperature at which propellant condensation will occur when such condensation presents a threat to the safe operation of the system.

Note: *Threats to safe system operation include condensation in pressure regulator sensing ports, lines which will be swept by high velocity pressurant, and condensation which could make a significant quantity of propellant unusable.*

4.8.2.8 **Propellant vapor migration** - Temperature control of propulsion hardware **shall** avoid temperature gradients that cause migration of propellant vapors when such migration presents a threat to safe operation of the system.

Example: In propellant tanks with elastomeric diaphragms, the time-averaged bulk temperature on the gas side is maintained higher than the time-averaged bulk temperature of the liquid.

4.8.2.9 **Power density limit for film heaters** - Film heaters, when bonded to a metallic or composite substrate, **shall** (*should* for Type II) be limited to a maximum power density according to the requirements of the JPL Derating Standard or alternate, approved, derating document for Type 0.

Type 0 projects **shall** document which derating document they will use in their approved Project Plan, if not the JPL Derating Standard.

4.8.2.10 **Maximum duty cycle of actively controlled heaters** - The maximum duty cycle **shall** be 80% or less under worst-case cold environmental conditions when actively controlled heaters are implemented in a flight system thermal control design.

Type 0 projects **shall** document alternative duty cycle, if different, in an approved Project Plan, in lieu of writing a waiver.

Note: *The purpose of this requirement is to ensure that positive heater control authority exists during the design phase of the flight system thermal control. Heater duty cycling can fall outside of the prescribed design range during the mission, but should generally meet the above maximum duty cycling criteria during ground testing to validate the thermal control design.*

Note: *This principle applies to systems above -70 degrees C. Active controllers include mechanical thermostats and Proportional-Integral-Derivative (PID) or pulse wave modulated controllers. To conserve power consumption throughout the mission due to typically large spacecraft bus voltage ranges, the maximum 80% duty cycle applies to the condition of a minimum nominal voltage,*

and not a minimum failed voltage, e.g., failed battery cell or solar cell string.

4.8.2.11 **Cryogenic Design Margin** - The total power load margin for passive coolers, mechanical coolers and stored cryogen systems designed to operate below –70°C **shall** be greater than 25%, as determined by Qual/PF and Flight Acceptance (FA) testing.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Rationale: Small additional detector heat loads in the range of a few milliwatts to tens of milliwatts (both active and parasitic) can have large adverse thermal impacts on some cryogenic systems. Margins are protection for uncertainties and modeling errors on a cryogenic system with a large thermal sensitivity. This requirement provides design robustness for cryogenic systems operating below -70 degrees C.

Note: *The cryogenic margin is to be used in conjunction with the realistic (non-anomalous) stacked worst-case thermal analysis of the cryogenic system enclosure and adjacent spacecraft hardware.*

Note: *See 6.3.10 for margin definition, and margin limits at key development milestones.*

4.8.2.12 **Motor and actuator self-heating** - Motor or actuator operating AFT and qualification/protoflight temperature ranges **shall** be defined by the interface or environmental temperature extremes, prior to energizing a motor or actuator, with the maximum allowable temperature limit of the motor or actuator due to self-heating separately defined.

Rationale: This requirement is to ensure consistency between the definition of operating and non-operating Allowable Flight Temperature limits, while accommodating the characteristic of motor or actuator self-heating during ground testing.

4.8.2.13 **Test limit-to-hardware capability limit margin** - When the hardware capability temperature limit is known and presents a hard constraint on the thermal control design, the qualification/protoflight temperature limit **shall** be chosen to provide a minimum of 10 degrees C margin to the hardware capability temperature limit.

For example: Temperature limits of hardware capabilities occur when essential mechanical clearances are reduced to zero, or

component materials reach their maximum usable temperature, or the manufacturer's limit above (or below) which component operation is not guaranteed. With respect to electronic parts, hardware capability limit refers to the manufacturer's component specification upper and lower temperature extremes, and not the end-user de-rating requirements.

4.9 System Fault Protection Design

4.9.1 General

4.9.1.1 **Fault protection definitions**- Definitions used in the Fault Protection section are as follows:

a. Anomaly- any unexpected occurrence.

Note: *Applied to indicate any of faults, failures, and their observable symptoms*

b. Error- an observable symptom of a fault

Note: *In not all cases will faults give rise to observable symptoms.*

c. Failure- the inability of a system or component to perform its required function.

d. Fault- a physical defect or occurrence which causes the loss of required functionality

4.9.1.2 **Protection for credible single faults** - Fault Protection **shall** (*should* for Type II and Type 0) handle all credible single faults or losses of functionality within all expected environmental conditions.

Note: *Fault protection is not intended as a remedy for faults that result from design error and/or designs that are inadequate for the specified environment.*

Rationale: *Designs should not be required to handle unrealistic scenarios, yet based on our operational experience, we know they must handle 'unknown-unknowns'. Fault protection scope must include function preservation (loss of functionality) as well as identified fault scenarios. This notion of a 'safety-net' would include (but not be limited to) uplink command loss, attitude control loss, attitude knowledge loss, ephemeris errors, excess system momentum, system power/energy deficiency, and system over/under temperature.*

4.9.1.3 **Protection for multiple faults** - Fault protection **shall** (*should* for Type II and Type 0) handle multiple, non-coincident faults, provided that they occur in functionally independent system elements.

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

Note: *A newly discovered latent fault (e.g., one exposed by a recovery action for a recent fault) should not be considered a concurrent fault. Only the error detection is concurrent in this case. Operational mitigations to reveal latent faults in a timely manner may obviate the need to deal with such concurrent errors.*

4.9.1.4 **Smallest level of FP concern** - Fault protection **shall** (*should* for Type II and Type 0) be able to diagnose and isolate faults at the level of the defined fault containment regions, and need not attempt recovery below this level.

Note: *Fault containment regions represent the smallest level of concern to fault protection. See 4.12.1.6.*

Rationale: Redundancy schemes can be seriously compromised in the absence of fault containment. Also, failure to contain faults can complicate recovery by confusing diagnosis, and requiring more complex response actions.

4.9.1.5 **Tolerance to false alarms** - At all times throughout the mission, the spacecraft **shall** (*should* for Type II and Type 0) tolerate execution of fault protection in response to false alarms.

Rationale: False alarms are inevitable, so the system shouldn't be vulnerable to them.

Example: Incorrectly set monitor threshold may cause an unexpected response, and this should not severely degrade the mission, or create an operational hardship.

4.9.1.6 **Variation in FP behavior** - Variations in fault protection behavior **shall** (*should* for Type II and Type 0) be based directly upon the system mode or activity, rather than indirectly on individual manipulation of enables, thresholds, etc.

Example: Fault protection objectives or behavior may vary depending on mission phase. This variation should be based upon system modes or circumstances, rather than changed via a separate set of commands that alter fault protection enables/disables, thresholds, etc. System-wide behavioral changes should be made in a more atomic, integrated fashion- making the overall design less susceptible to operator error, or timing vulnerabilities.

4.9.1.7 **Speed of fault detection and response** - The fault protection **shall** (*should* for Type II and Type 0) be designed to respond in a timely manner to identified threats to flight system health, safety, and/or mission success.

Rationale: The fault response must complete within the time that the fault is detected and the time that the potential hazard would occur without any fault protection.

4.9.2 Fault Protection Response

4.9.2.1 ***Deleted***

4.9.2.2 **Flight system safing** - Following fault conditions that may impact spacecraft health, safety, or consumables, fault protection **shall**, at a minimum, autonomously configure the spacecraft to a safe, sustainable, ground commandable mode that preserves vital spacecraft resources and provides for at least an RF carrier downlink signal to the Earth.

Note: *The safing mode may be a single state or more than one state. The RF downlink signal need not be continuous, but must be predictable in its timing. For all post-launch mission phases, change all spacecraft state defaults to a post-launch state to ensure that the spacecraft will be able to enter a safe mode.*

Rationale: The spacecraft must autonomously recover from a detected fault when the function(s) affected by the fault threaten spacecraft/instrument survival (e.g., functions necessary to maintain Safe mode). Ensure spacecraft survivability and viability by preserving vital spacecraft resources (e.g., thermal, power), while enabling ground interaction (e.g., command and downlink) for recovery operations. It is not enough merely to diagnose and isolate faults, or to restore lost functionality, if the resulting system state still threatens the rest of the mission (e.g., through stress, loss of consumables, or unresponsiveness to operator control).

4.9.2.2.1 **Sustainable duration** - The safe state(s) established by the safing response **shall** be sustainable for a duration consistent with the frequency of planned communications contacts and timing of operational activities.

Note: *A missed tracking pass should not be reason to declare a s/c emergency, thus requiring rescheduling of tracking resources.*

Note: *14 days is a typical duration based on the interval between ground contacts, but can be project and mission phase dependent.*

4.9.2.2.2 **Fault protection during safing** - The spacecraft **shall** (*should* for Type II and Type 0) be able to detect and respond to faults while in a safe configuration including the safe state(s) established by the safing response.

Rationale: *Transition to safing may be due to an operational mistake, and the system should still be single fault tolerant while awaiting ground recovery.*

4.9.2.3 **Autonomous completion** - For events or activities that are required for mission success and must be performed without the possibility of ground intervention, fault protection **shall** (*should* for Type II and Type 0) endeavor to ensure the autonomous, timely completion of that event or activity.

Note: *Autonomous completion implies restoring the functionality needed to complete the mission-critical event. See 4.9.1.2 and 4.9.1.3.*

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

4.9.2.3.1 **Accommodation of processor resets** - The design **shall** accommodate processor resets during mission-critical events.

4.9.3 Flight-Ground Interface

4.9.3.1 **In-flight commandability** - The fault protection design **shall** (*should* for Type II and Type 0) permit ground operators to easily modify in-flight the fault protection control settings (e.g., enables, thresholds, persistence values).

Note: *The notion of easy modification connotes attributes including 1) causing minimal impact to operations 2) no reboot required and 3) no need to reassert values not being changed.*

Rationale: Ensures an operable design. Fault protection updates are always required, e.g., to adjust thresholds, persistence values, based on actual in-flight system performance. In-flight flight software reloads should not be required for these routine FP updates.

4.9.3.2 **Visibility into fault protection state** - The flight system **shall** have the capability to telemeter the status of all ground-commandable fault protection control settings.

Rationale: Visibility provides operators with the most reliable means of knowing the current state, and minimizes the potential for improper settings.

4.9.3.3 **Control of fault protection control settings** - Fault protection **shall** (*should* for Type II and Type 0) enable ground operators to assert fault protection control settings in such a manner that those settings cannot be autonomously changed.

Rationale: Avoids the vulnerability of being in an undesired configuration, which could occur if on-board events could un-do the ground settings.

Example: The design allows ground operators to disable a response in such a way that the response cannot be autonomously re-enabled.

4.9.3.4 **S/C state information** - The fault protection design **shall** ensure that monitors reflect the current condition of the spacecraft. (e.g., be sure to clear stale symptoms and don't work off of stale data).

Rationale: Responses to stale data will inevitably lead to errors in the fault protection behavior.

Note: *It is very important to respond to the current state of the spacecraft rather than a past state. Allows the ability to re-enable responses without inadvertently tripping per stale data.*

4.9.3.5 **Fault protection margin monitoring** - The flight system **shall** provide insight into fault protection monitoring to determine margins against thresholds and persistence values.

Note: *An example would be the ability to telemeter high water marks, which indicate the maximum values and persistence values of the error symptoms that are autonomously monitored by fault protection.*

Rationale: Reducing the likelihood of false alarms requires insight into system behavior relative to fault protection expectations. Margin monitoring provides insight into the fault protection performance to be able to determine 'how close is the fault protection to tripping.' This knowledge is invaluable to detect threatening conditions before they impact the system, and enable the ground to properly 'tune' thresholds and persistence values, ensuring unintended fault protection tripping can be avoided.

4.9.3.6 **Fault reconstruction data** - The fault protection design **shall** provide telemetry that allows ground operators to reconstruct its autonomous actions, and to locate a failure accurately enough to support ground-based diagnosis and redundancy management.

Rationale: Such data is essential for understanding the cause of the response, the resulting state of the system and any threats to it, and the steps that might be necessary to restore operation, and avoid future problems.

4.9.3.7 **Visibility into fault response activity** - Without the need for initiation by a ground command, the spacecraft **shall** telemeter the basic status on whether and how fault protection has responded to a fault condition.

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.

4.9.4 Fault Detection

4.9.4.1 **Fault indication filtering** - The fault protection **shall** be designed to respond only to those symptoms that pose a potential threat to flight system health and safety, and/or mission success.

Rationale: Responding to mere performance problems, instead of actual threats, may result in fault protection response actions

such as unnecessarily perturbing operations, power cycling equipment, and bringing un-calibrated hardware online.

Note: *Don't respond simply because system performance is unexpected or out of specification. This will make the fault protection much more vulnerable to false alarms. Instead, respond because system performance is "unacceptable". "Unacceptable" can be defined as that which poses an immediate threat to health & safety and/or mission success.*

A balance must be achieved between two objectives. One is setting trigger values high enough to avoid premature (i.e., "hair") triggers. The other is to react early enough to avoid serious impacts to the mission, and/or spacecraft health and safety. Designing capable fault monitors that can distinguish between the 2 competing considerations effectively addresses this concern.

4.9.4.2 **Deviation from expected behavior** - Fault protection **shall** respond both to error indications and deviation from nominal behavior, when a significant threat to mission/system integrity is indicated.

Rationale: Not all possible faults or failure modes can be anticipated or always detected, therefore the system should also assess significant deviation from nominal behavior for indication of faults, and respond appropriately.

4.10 System EMC/EMI Design

System EMI/EMC refers to the highest level of assembly. However, Engineering Delivery Tasks (EDTs) limit the scope of work to partial systems and do not include authority over higher level system decisions. Therefore, this design control only applies to the extent possible within the scope of work context.

4.10.1 **General**

4.10.1.1 **EMC approach** - The grounding and interfacing design **shall** provide for an equipotential spacecraft, including, when needed, a "Faraday" cage. Also the grounding and interfacing design *should*:

a. Provide low conducted and radiated emissions

b. Provide high transient noise immunity on circuitry,

c. Prevent or minimize external and internal Electrostatic Discharge (ESD),

d. Provide for magnetic field cancellation within each harness bundle, and

e. Prevent DC currents from flowing through structure.

4.10.1.2 **Minimizing EMI** - Grounding and interfacing ***should*** be implemented in the electrical and mechanical design (including packaging) to minimize Electromagnetic Interference (EMI). For example, when magnetic cleanliness is a design driver, magnetic field cancellation ***should*** be provided within solar array segments.

4.10.2 **Grounding and Interfacing**

4.10.2.1 **Local single point ground** - Each subsystem ground tree (i.e., power converter secondary) **shall:**

a. Have a local single point DC ground to spacecraft chassis with the lowest possible impedance (including high speed balanced digital interfaces), except interfaces greater than 200V DC or peak AC.

b. Be grounded to chassis at source and load end for interfaces greater than 200V DC or peak AC.

c. Have a common signal ground and chassis ground in the frequency range of 300 kHz – 3 THz (RF and high speed unbalanced digital assemblies).

Rationale: Principle: Ground loops shall be avoided to prevent un-desired radiation from wiring and other interconnects, and the creation of offset voltages which affect the operational integrity of a circuit and cause errors in data interfaces.

Case a) The simplest and most effective way to avoid the creation of ground loops is to connect each ground path in circuits powered by a power converter secondary to a single ground point.

Case b) Single point ground is not possible for RF since RF and DC currents take different paths. RF currents flow through the case of most RF circuit elements, and is returned through the local chassis impedance. Coaxial interconnects between RF assemblies inherently introduce multi-point grounding, since each RF chassis is grounded to the spacecraft structure, and also to other RF chassis via the interconnecting coaxial cables. Unbalanced high-speed digital interfaces have the inherent multi-point grounding as RF, since the transmitter is grounded locally and likewise the

receiver, which may be on another power converter secondary with a common ground reference.

Case c) High voltage circuits have special safety consideration given the large fault currents possible. The principle for high voltage interfaces is to provide a local fault current return to chassis to avoid circulating large fault currents over an inter-connect. There are two reasons for this: first, large fault currents will radiate from interconnection wiring and interfere with other spacecraft elements; second, large fault currents flowing through any significant interconnect impedance will raise the local potential of the faulted assembly in a transient manner to damagingly high voltages.

4.10.2.2 **Power interface hot-to-return separation** - Power hot and return, and chassis functions, **shall** be adequately separated to preclude the possibility of hot-to-return or hot-to-chassis shorts. The conductors **shall** reside within the same connector and within the same harness bundle.

Note: *The separation may be implemented by recessed contacts. Conductor co-location provides for magnetic field cancellation.*

4.10.2.3 ***Deleted***

4.10.2.4 ***Deleted***

4.10.2.5 ***Deleted***

4.10.2.6 **Slip rings** - Electrical signals (including primary power) routed through slip rings **shall** be immune to arcing and short circuits between adjacent conductors in the slip ring assembly.

Rationale: Over time debris can be generated and bridge between adjacent conductors.

4.10.3 **Control of Emissions**

4.10.3.1 **Shielding potential sources** - High current, high di/dt and dv/dt interface wires **shall** be appropriately shielded/grounded.

4.10.3.2 **Separate routing for pyro circuits** - Pyro firing interfaces **shall** be routed separately from other interfaces, and **shall** use separate connectors consistent with Mission Range Safety Requirements.

4.10.3.3 **Electromotive Force (EMF) suppression for inductive loads** - Inductive loads (e.g., valve coils, relay coils, and motor windings) **shall** be equipped with back-EMF transient suppression.

4.10.3.4 **Routing of signal and return wires** - The routing of signal and return wires **shall** provide for magnetic field cancellation as required for flight system electromagnetic compatibility.

Note: *Signal and return wires (including power and return wires) are to be routed as closely together as possible in order to achieve magnetic field cancellation.*

Rationale: Stray magnetic fields may cause EMI problems.

4.10.4 **Control of Susceptibility**

4.10.4.1 **Primary circuit return path** – Wires, except for coaxial circuits, **shall** be used instead of structure or shields for the primary circuit return path.

4.10.4.2 **Wire treatment** - Wire treatment (shielding, twisting, wire type, etc.) applied to electrical interfaces routed in system cabling **shall** provide >6 db margin for proper operation of the interface under worst case conditions (e.g., worst EMI environment, temperature, voltage, aging).

Note: *>6 db margin exists when the margin to proper operation of the interface is reduced less than half by the effects of the wire treatment. For example, noise coupled to signal interfaces, voltage drop in power interfaces, and timing skew in data interfaces reduces the margin for proper operation by half from that which exists in the absence of coupled noise, voltage drop, and timing skew respectively.*

4.10.4.3 **Immunity to expected transient circuit interruptions** - Electrical signals (e.g., data, timing, power, circuit returns) that use flex cable designs or that cross mechanical articulating or rotating assemblies (e.g., slip rings) **shall** be immune to transient signal interruption.

4.10.4.4 **Immunity to simultaneous pyro firings** - If the pyro firing system (power source, switching elements, system power bus) connects to six or more NASA Standard Initiators (NSIs), the design **shall** operate properly through simultaneous firing of up to six NSIs under worst-case conditions (e.g., temperatures, voltage, etc.). If a pyro bank connects to fewer than six NSIs, the design **shall** operate properly through simultaneous firing of all its NSIs under worst-case conditions (e.g., temperature, voltage, etc.).

4.10.4.5 **Use of filtering** - When the potential exists for spurious signals on system electrical interfaces to initiate an unintended response that could be mission catastrophic, filtering (consistent with bandwidth requirements) **shall** be provided in the receiving end-circuit to minimize the threat.

4.10.5 Control of Electrostatic Discharge

4.10.5.1 **Use of Static Bleed Path** - Isolated circuitry that relies on system cabling to provide its ground reference **shall** include an internal (to the assembly) bleed path to local chassis not to exceed 100 Meg ohms.

Note: *Applicability is to isolated circuitry exceeding 100 Meg ohms to chassis, and greater than 15 cm in length and/or greater than 3 sq cm in net surface area.*

Note: *A 20 Meg ohm resistive path to chassis is recommended.*

Rationale: Prevent charge buildup during periods when the unit is not mounted to the spacecraft and/or is disconnected from the cabling that provides the ground path.

Note: *Legacy hardware with 1 megohm static bleed resistive path to assembly structure may be acceptable, but requires a system-wide assessment of the potential impacts associated with paralleled bleed resistors.*

4.10.5.2 **Ungrounded conductors** - Space-exposed or “spacecraft-buried” ungrounded conductors **shall** be demonstrated to not pose an ESD disruption or damage threat by avoiding ungrounded (floating) conductor > 15 cm in length.

4.11 Flight Software System Design

4.11.1 General

4.11.1.1 Software architectural design

4.11.1.1.1 Documentation of architecture design

The documentation of the architectural design of a software system **shall** (*should* for Type II and Type 0):

a. Identify and describe the architectural elements of the software, the external interfaces, and the interfaces between elements.

b. Include element responsibilities (constraints on inputs and guarantees on outputs), and constraints on how the elements interact (such as message and data sharing protocols).

Note: *The architectural elements are the high-level elements, often composed of smaller elements. Examples of architectural elements are: a software message bus, a command processor, a device driver.*

Interfaces are ways in which entities can affect each other. External interfaces are ways in which the software system can affect its environment or the environment can affect the software system. In systems where safety critical and non-critical functionality are needed, the use of hardware and operating system capabilities to partition the elements should be considered in the architecture.

4.11.1.1.2 **Architectural analysis of quality attributes**

The architectural design documentation **shall** (*should* for Type II and Type 0) include multiple views of the architecture and identify and support the evaluation of the key quality attributes of the planned software product.

Note: *The key quality attributes of the software will depend on the mission in which the software is to be used and the manner in which the software is to be developed and deployed. They will usually include: performance, availability, maintainability, modifiability, security, testability and usability (operability.)*

4.11.1.2 ***Deleted***

4.11.1.3 **Semantics of data interfaces** - The semantics of data conveyed across public interfaces, whether inside an executable or as input to or output from an executable, **shall** be clearly specified and, if possible, verified in an automated way at build time.

Note: *Data semantics may include range, precision, physical units of measure, and coordinate frames, as applicable.*

Rationale: *The principal risk is miscommunication between engineering teams about the meaning of data conveyed across major public interfaces. It's not enough to specify semantics in an*

interface control document and rely on human inspection. This principle presumes that elements developed by an individual programmer, or within a cohesive team are more likely to be self-consistent, whereas external interfaces are less likely to be consistent.

Applicability: This principle applies primarily to public interfaces that cross system, subsystem, or component boundaries --- specifically, boundaries between software elements developed by different programmers. The importance of critical (formal) verification of these interfaces should be commensurate with the organizational separation between developers on each side of the interface.

4.11.1.4 **Compatibility with COTS tools** - Where commercial hardware, operating systems, or other tools are used to support testing, flight software **shall** be designed to operate on such platforms with little change, such that these tests are substantially relevant to software V&V.

Note: *This is to support unit testing and early integration testing, and to lessen dependency on high fidelity hardware-in-the-loop testbeds.*

4.11.1.5 **Demonstrable correctness properties** - The software *should* have demonstrable correctness properties, supported by evidence from the use of appropriate static analysis techniques.

4.11.2 Initialization

4.11.2.1 Nominal flight software initialization

Flight software **shall** be designed to initialize software and hardware to a known, safe, and deliberate state.

Note: *Elements to consider when establishing state include inertial, temporal, device capability or configuration, file allocation tables, and boot code in RAM.*

4.11.2.2 Multiple restart flight software initialization

The software **shall** (*should* for Type II) be designed to detect off-nominal restarts and to successively reinitialize with less and less dependency on preserved state (e.g., inertial, temporal, device capability or configuration, file allocation tables, boot code in RAM…) from before the most recent reset, until a fully known and tested initial configuration is obtained, and until stable operation has been restored.

Note: *Reset is commonly used as a means of autonomous recovery from serious software problems caused by errors or single event upsets. Reset is not effective unless the problematic software state is cleared during re-initialization. Ultimately, all software states must be presumed suspect and expendable, if prior re-initializations have failed to resolve a problem. A complete accounting of preserved state is essential, if effective measures are to be taken against it.*

4.11.2.3 **Minimalist boot**

The boot implementation of the flight computer(s) software **shall** (*should* for Type II and Type 0) include a "minimalist" configuration that requires a minimum of on-board resources for vehicle safety and ground intervention.

Note: *This 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 that was capable of minimal operations without the file system.*

4.11.2.4 **System initialization trace telemetry**

The flight software **shall** (*should* for Type II and Type 0) be designed to record and transmit its progress through each attempt at initialization.

4.11.3 **Interfaces**

4.11.3.1 **Use of standards** - Flight software **shall** employ applicable JPL and JPL sanctioned standard products (including data formats, interface specifications, and software designs) and standard processes, procedures, practices and methods in the development and testing of software systems.

Rationale: Standards represent consensus solutions for recurring situations as agreed to by parties with vested interests in the subject matter.

Artifacts: Specification in software design documents and models of applicable standards. Reference to controlling standards in Software Measurement (or Management) Plan/Software Development Plan (SMP/SDP) and Software Integration and Test Plan (SITP) or Verification and Validation Plan (VVP). Compliance verified through reviews.

4.11.3.2 ***Deleted***

4.11.3.3 Parameter and argument specification

a. Parameters and interface function arguments **shall** be specified in terms of their attributes.

Rationale: To prevent computational errors as a result of interface errors.

b. Physical units of measure and reference frames **shall** be specified and checked for consistency (automatically where possible).

c. Additional attributes **shall** include but not be limited to:

i. Derivation or origin of parameters so that they can be maintained and dependencies with other parameters are visible,

ii. Parameter type such as enumeration, alphanumeric, floating point, integer, etc.,

iii. Nominal value, precision, accuracy, and allowable range for numeric types,

iv. Other specific attributes for non-numeric types such as organization and format.

4.11.4 Design Robustness

4.11.4.1 *Deleted*

4.11.4.2 Response to incorrect commands, loads, data, or memory

a. Flight software **shall** be designed to detect and respond safely to corrupted commands, data, or loads, and memory faults allocated to the software, such as stuck bits or Single Event Effects (SEE).

Note: *For example, flight computer designs have included Error Detection And Correction (EDAC) logic on EEPROMs, and the load process has been designed to detect and respond to failure if the EDAC detects an uncorrectable bit error. Software designs have included check sum logic and periodic verification of memory to detect command, data, or load, and memory faults.*

b. Flight software **shall** be designed to detect and respond safely to commands, data, or loads, that are incorrectly formatted, including invalid values, or out of range parameters.

c. Flight software **shall** be designed to detect and respond safely to commands, data, or loads that are invalid in the current context.

Note: *For example, a command handler should check whether a received command is appropriate for the current system mode, and a software module should check whether a*

command is appropriate for its local state, or out of order in the current context. Paragraph 4.11.4.2 (c) does not apply to commands, data, or loads where the consequences are clearly insignificant.

4.11.4.3 **Protection from unintended software modification** - Flight software that is modifiable during flight **shall** be protected from unintended modifications including those caused by operations errors, single event effects, and hardware problems.

Note: *Protection is typically provided by intentionally enabling a write operation before modifying the software; at all other times, write operations are disabled to protect the software from unintended modifications. Unintended modifications can be introduced through configuration management, design, and operations flaws as well as physics.*

4.11.4.4 ***Deleted***

4.11.4.5 **Response to resource over-subscription** - The software design **shall** contain a robust response to situations where computer resources are oversubscribed. The action to be taken in such situations **shall** be specified as part of the requirements on the design.

Note: *Examples of these situations include buffers overflowing, exceeding a rate group time boundary, and excessive inputs or interrupts. There are several common methods for tolerating these situations, most of which relate to reducing demand from non-essential items, especially if they are the source of over subscription:*

a. Generate warning messages when appropriate.

b. Instruct external systems to reduce their demands.

c. Lock out interrupts.

d. Change operational behavior to handle the load. For example, the software may use faster but less accurate algorithms to keep up with the load.

e. Reduce the functionality of the software, or even halt or suspend a process or shutdown a computer.

4.11.4.6 **Response to input/output anomalies** - Software **shall** be designed to tolerate and continue functioning in situations where periodic and/or regular inputs are temporarily missing, or Input/Output (I/O) fails to complete, completes unsuccessfully, or is invalid.

Note: *An example of this situation is resorting to dead reckoning for navigation as long as navigation measurements are not available from hardware.*

Input/output completion time-outs are often used to detect a failed input/output transaction and restore continuity.

When writing to output, it is often good practice to read it back to verify that the write completed successfully.

Software should accommodate both nominal inputs (within specifications) and off-nominal inputs, from which recovery may be required.

4.11.4.7 **Use of time-outs** - Software **shall** be designed to detect and respond appropriately to failures to complete required activities on time.

Note: *Watchdog timers are commonly used for this purpose. Upon completion of a defined processing path, the software resets a watchdog timer. If the processing gets lost, or fails to make progress, the timer times-out. The timer directs the software to a known point where the processing is restored.*

4.11.4.8 ***Deleted***

4.11.4.9 ***Deleted***

4.11.4.10 ***Deleted***

4.11.4.11 **Protection against incorrect memory use** - Software **shall** (*should* for Type II and Type 0) be designed to protect against incorrect use of memory:

a. Execution in data areas, unused areas, and other areas not intended for execution caused by branching into non-code areas.
b. Using code as data.
c. Unintended, harmful over-writing of code areas.

Note: *Wherever possible, features of the processor, operating system, and the surrounding peripheral hardware should be utilized to protect against incorrect memory use. For example, enabling the "page write protection" control bits such that writing to protect memory areas causes interrupts. Software techniques may also be used such as:*

a. *Initializing unused memory to illegal instructions that cause interrupts when executed.*

b. *Background checking of the integrity of the image load to confirm that it has not been corrupted*

c. *Memory boundary checking of external Direct Memory Access (DMA) engines to prevent overwrite of inappropriate regions of memory.*

d. *Use of currently available hardware and operating systems capabilities, including partitioning, should be also considered in the design.*

4.11.4.12 **Data set consistency** - Software **shall** (*should* for Type II and Type 0) be designed to ensure that data sets and parameter lists are consistent when passed among threads such that data is known to be complete when used, and that there is no danger of using a mixture of old and new data.

Note: *For example, software should not be interrupted in a manner that permits it to use both old and new components of a vector.*

4.11.4.13 **Thread-safe operations** - Software **shall** (*should* for Type II and Type 0) be demonstrated via test and/or analytical methods to be free of deadlocks, failures to make progress, race conditions, and other threats to multi-threaded operations.

Note: *A deadlock is the condition where two processes cannot proceed because each is waiting to use a shared resource held by the other.*

A race condition is anomalous behavior due to unexpected critical dependence on the relative timing of events.

Non-progress cycles exist if a potentially infinite execution cycle does not include a state indicating that progress is being made.

Thread-safe is defined as code which functions correctly during simultaneous execution by multiple threads

Model-based techniques are recommended wherever possible as a means of demonstrating compliance with this requirement.

4.11.4.14 **Software managed state transitions** - The flight software design must not introduce unintended or unspecified side effects in the implementation of system and software state machine logic. In particular, the design **shall** (*should* for Type II and Type 0) avoid

uncertain, unsafe, or hazardous consequential states during software managed state transitions.

Note: *Careful design of state machine logic and similarly careful software implementation will avoid unintended side effects. In practice, this means that the software design must account for all the steps that must be performed during a transition as well as the time it takes to perform those steps. Furthermore, the Flight Software (FSW) design overall must not allow for any indeterminate configurations to exist during the transition between states. In practice this usually requires detection of incomplete or interrupted transitions and the reinforcement of a known configuration.*

4.11.5 **Verification**

4.11.5.1 ***Deleted***

4.11.5.2 **Design for incremental verification** - The design **shall** enable easy software testing at unit, module, subsystem test bed and system test bed levels to incrementally verify functionality/operability. This includes regression testing.

Note: *Techniques known to improve the ease of testing include code modularization with low coupling, error injection mechanisms, code test instrumentation, uniform test case specifications, and uniform test harnesses.*

4.11.5.3 ***Deleted***

4.11.5.4 **Stress testing** - Software algorithms and their implementation **shall** (*should* for Type II and Type 0) degrade with understandable behavior when stressed beyond their performance limitations. Some examples include:

a. Being sensitive to identified uncertainties
b. Precluding an undesired response to mathematical singularities or limitations
c. Responding predictably to possible events that exceed capabilities.

4.11.6 **Diagnostic and Self-Test Capability**

4.11.6.1 **Self-test capability** - The software design **shall** (*should* for Type II and Type 0) include capabilities to test operation and permit timely fault diagnostics.

a. **If not removed for flight** - If not removed, the test capabilities **shall** avoid (*should* for Type II and Type 0) causing flight hardware damage or interference with proper operation of the flight software if inadvertently executed in flight.

b. **If removed for flight** - If removed, the regression test baseline **shall** (*should* for Type II and Type 0) be rerun, and V&V testing performed after the removal.

Note: *Examples of test capabilities include, testing the underlying computing hardware, production of diagnostic traces, hooks for debuggers, introspection capabilities, instrumentation of performance or resource use, simulations for closed loop control, and special modes that support scripted I/O test.*

4.11.6.2 **Fault diagnostics** - Test/diagnostic code **shall** (*should* for Type II and Type 0) be designed and incorporated into the software early, and be 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.

Note: *In order to get the most benefit from it, the test/diagnostic code should be designed by PDR, and incorporated into the software by Critical Design Review (CDR).*

4.11.6.3 **Measurement of constrained resources** - Software **shall** (*should* for Type II and Type 0) be designed to provide easy and timely visibility into the use of computing resources during testing and operations.

Note: *Examples of resources to measure are: real time tasks, background tasks, throughput, memory, bus utilization, stack size and headroom, cycle slip statistics, fragmentation, memory leaks, and allocation latency.*

This makes it possible to validate margins and makes the flight software resource usage testable.

4.11.7 **Flight Software Margins** - See Section 6.3.5

4.12 Flight Electronics Hardware System Design

4.12.1 General

4.12.1.1 **Design partition** - The design **shall** be partitioned for implementation in a manner to preclude single failure modes (e.g., thermal, structural, etc.) common to both prime and redundant units of a subsystem.

4.12.1.2 ***Deleted***

4.12.1.3 ***Deleted***

4.12.1.4 ***Deleted***

4.12.1.5 **Radiation Design Factors (RDF)** - The design **shall** meet an RDF of at least 2 through to the end of the primary mission, for cumulative dose to parts.

Definition: Radiation Design Factor (RDF) = electronic part capability/electronic part expected local environment.

Rationale: Covers systematic uncertainties in environmental model and intrinsic environment variability.

4.12.1.6 **Fault Containment Regions**

Definition: A fault containment region is a segment of the system, the design of which is such that faults internal to the fault containment region do not propagate beyond the limits of the fault containment region.

Note: *Fault propagation can be both direct/obvious (e.g., damage, disabling) and indirect/subtle (e.g., contention, interference).*

4.12.1.6.1 **Subsystems and redundant units** - All electronic subsystems and redundant units within electronic subsystems **shall** (**not** required for Type II) be designed to be fault containment regions.

Note: *Fault containment is routinely implemented below the subsystem level when warranted by fault statistics, and is an efficient application in the overall system fault protection architecture, e.g., EDAC applied to memory.*

4.12.1.6.2 **Auxiliary circuits** - The design **shall** (*should* for Type II and Type 0) ensure that faults in auxiliary circuitry do not propagate to functional elements essential for mission success, e.g., failure of a telemetry monitor circuit propagates to the functional element whose performance is being monitored.

4.12.1.7 ***Deleted***

4.12.1.8 **Use of Fuses**

4.12.1.8.1 **Fuse utilization** - The use of fuses in mission-critical applications ***should*** be minimized.

Rationale: There is no recovery from an in-flight blown fuse, thus their use in mission-critical applications must be carefully considered.

4.12.1.8.2 **Fuse accessibility** - When used, fuses ***should*** be easily accessible for replacement and/or for integrity verification at any time prior to launch vehicle integration.

4.12.1.8.3 **Fuse sizing** - When used, fuses **shall** be sized to accommodate with margin- after consideration of temperature, aging, and operating environments, i.e., in air and in vacuum- the more stressful of the steady state and transient in-rush conditions.

Note: *Margin should consider the consequences of loss of functionality, the system's capacity to deliver the current required to blow the fuse, and the uncertainty in fuse characterization data.*

4.12.2 **Electronic Packaging**

4.12.2.1 **Thermal cycle life qualification of electronic packaging designs** - Electronic hardware **shall** be capable of surviving thermal cycle environments that are three times the service life, which includes the planned preflight ground testing environments, worst-case expected mission cycles with worst-case flight temperature excursions, operational self-heating, and power on-off temperature cycling. In the absence of specific mission thermal cycling profiles, electronic hardware **shall** be capable of surviving an equivalent thermal cycle life of 200 cycles with a temperature range of 155° C.

Note: *Verification of thermal cycle life qualification of electronic hardware packaging, including inherited and new designs and residual hardware items, is by test and/or analysis with test the preferred approach. When inherited designs and/or hardware are planned, the previous application and history are used to evaluate the new mission/system application. Package qualification and verification process flow, and roles and responsibilities for thermal cycle life of electronic packaging are established in Package Qualification and Verification Process Flow, Roles and Responsibilities.*

Rationale: Before committing to a new design or to the use of inherited designs or application of residual hardware, it is necessary to understand the thermal-cycle capability of the hardware being considered. In the absence of a mission and system requirement, it is prudent to use the thermal-cycle specification noted in 4.12.2.1. The specification of 200 cycles with a temperature range of 155° C originated from NASA Handbook Requirements for Soldered Electrical Connectors 5300.4(3A-1), which is now obsolete.

4.12.2.2 ***Deleted***

4.12.2.3 **High voltage designs** - Electronics with high voltage **shall** be designed and/or operated to prevent arcing and discharges, or failing that, then the system design **shall** be proven to operate properly in the presence of arcing and discharges.

Rationale: Arcing presents a risk to personnel, the flight hardware, and the integrity of the system design by virtue of the EMI it creates.

4.12.3 **Digital Design**

4.12.3.1 **Synchronous design** - Digital logic circuits, except reset circuits (see 4.12.3.2), **shall** be designed to operate synchronously to ensure proper logic timing. Where asynchronous exceptions are needed for valid design reasons, these **shall** be analyzed and tested to guarantee correct operation under worst-case conditions, and documented.

4.12.3.2 **Asynchronous reset signals** - Reset circuits **shall** be designed such that they are applied asynchronously and released synchronously.

Rationale: Circuit designs can have unpredictable states and outputs before on-board clock circuits are initialized. Asserting the reset signal asynchronously will force the internal circuitry and I/O to a known state.

4.12.3.3 **High-speed signal integrity** - When timing is critical, e.g., in the design of high speed digital circuits, the design **shall** take into account the analog character of the signals, and verification **shall** ensure the electrical integrity of the signals over the operating extremes, e.g., temperature, voltage, etc.

Rationale: Analog signal integrity of digital circuits is critical for proper electrical performance of bus signals and other timing sensitive circuits.

Note: *Verification becomes more important as logic signal levels are smaller in amplitude.*

4.12.3.4 **Design of Field Programmable Gate Arrays (FPGAs)** - FPGAs **shall** be designed in accordance with the standard, Field Programmable Gate Array Development Process.

4.12.4 **Analog Design**

4.12.4.1 ***Deleted***

4.12.5 **Interfaces**

Note: *Also see 4.1.6*

4.12.5.1 **Flight-support equipment interfaces** - Support equipment (ground handling and test equipment) interfaces with flight hardware **shall** be designed to preclude test operator/test equipment or environmentally induced damage or degradation to flight hardware, e.g., via protective over-voltage, over-current or over-pressure devices.

Rationale: Reduce the possibility of flight hardware damage or degradation due to Test Operator errors, Support Equipment faults, or undesired environmental excursions.

4.12.5.1.1 **Lightning suppression** - Flight hardware **shall** be protected from lightning on electrical interfaces with ground support equipment at the launch site.

4.12.5.2 **Test circuits** - Electronics circuits resident on flight subassemblies used solely during test **shall** (**not** required for Type II, *should* for Type 0) be precluded from interfering with flight functionality by:

a. being exclusively powered by the support equipment and isolated from the flight circuitry; or by

b. being powered by flight power that is inhibited when the support equipment is disconnected thus leaving flight resident test components unpowered; or by

c. not populating test circuits on Flight Model boards.

Rationale: Allowing test circuits to interfere with flight circuits is undesirable. Test-only circuits are properly understood to be a subset of ancillary data functions, and as such, must be designed to not interfere with flight functionality.

Note: *Isolation of test circuits that receive their ground reference from the support equipment is only typically realized at dc, and is affected by the resistive bleed paths included in flight equipment for control of static charge build-up. See 4.10.5.1. Typical isolation will be in the range of a few hundreds to a few thousands of Kohms.*

4.12.5.2.1 **Test circuits/Flight circuit Interface Sharing** - Circuits resident on flight subassemblies used solely during test **shall** (*should* for Type II and Type 0) route test interface functions exclusively through parts and connectors dedicated to test functionality.

Rationale: Not sharing interface parts between flight and test functionality reduces the probability of fault propagation from test functionality to flight functionality. Keeping test circuitry on separate connectors, limits the possibilities for fault propagation and damage due to test related cable issues being improperly coupled to flight functions.

4.12.5.3 **Test access** - Test access **shall** be provided for verifying successful mating of connectors for all electrical interfaces that cannot be functionally verified after final mating, e.g., pyro circuits, propulsion actuators, deployable devices, safety interlocks, etc.

4.12.5.4 **Connector mis-mating** - Connectors **shall** be labeled with a unique identifier. To protect against incorrect mating of connectors, best practice is to implement unique mechanical features (connector type, keying, shell gender or pins/sockets gender) of adjacent connectors within the extent of the cable service loop (cable bundle slack). When this is not practical due to volume restrictions or limited available connector configurations, multiple workmanship assurances (at least two) **shall** be implemented in the drawing and/or assembly procedure to ensure proper mating: cable bundle forming, double QA check-off, additional labeling, and/or color coding.

Rationale: These requirements are to protect against the incorrect mating of connectors through human error. However, the necessary density of hard-mounted connectors for Mars landed missions, and usage of miniature connectors that are not available with different shell configurations, have resulted in an inability to implement the best practices of the Note below.

Note: *Connector orientation, labeling and color-coding may provide added protection against mis-mating of connectors, but are not as robust protection as are connector uniqueness and limiting the cabling service loop lengths.*

4.12.5.5 **Restricted usage** – Due to poor reliability history:

a. Reed switches **shall** only be used in non-critical applications.

b. Microswitches alone **shall** be avoided to initiate on-board autonomous activities where hardware damage or unsafe spacecraft operating conditions may result.

c. Opto-coupler use **shall** be limited to environments where radiation effects are tolerable.

4.12.5.6 **Separation interfaces** – Functions that pass through separation connectors (e.g., umbilical and direct access circuits) **shall** be protected in the event of inadvertent connection (singly or in combination) between any conductor and any other conductor (including spacecraft chassis) for any interface having a remaining mission function.

Note: *The protection afforded ensures that s/c functions having a remaining mission use will be unaffected by inadvertent connection(s) at the separation interface.*

4.12.5.7 **Deadfacing** –

a. **Before cable cutting** - Electrical interfaces (signal and return) passing through cable cutter separation devices **shall** be deadfaced prior to actuation of the device, e.g., signal and power interfaces are unpowered.

b. **After cable cutting** - Following cable cutter actuation, circuit grounding **shall not** result in violation of the single point ground principle on any ground tree having a remaining mission function.

Note: *Deadfacing is achieved when no current will flow into (or from) chassis should the cut wires come in contact with chassis.*

Rationale: *Conductor-to-conductor and conductor-to-frame short circuits are possible as a result of cable cutter activation in normal operation.*

4.12.6 **Flight Electronics Thermal Design**

Note: *Temperatures are established at the mounting or thermal control surface for the specified assembly.*

4.12.6.1 **Silicon piece part junction temperatures** - The thermal design of electronic assemblies **shall** maintain piece-part silicon maximum junction temperatures within the derating guidelines of JPL Derating Standard or alternate, approved, derating document for Type 0, given the assumption (for Type I) of a mounting surface temperature at the max (upper) Qual/PF temperature limit or +70°C whichever is greater. For Type II and Type 0, the assumption is of a mounting surface temperature at the max (upper) Qual/PF temperature limit.

Type 0 projects **shall** document which derating document they will use in their approved Project Plan, if not the JPL Derating Standard.

Note: *Long life and high reliability are enhanced by maintaining piece part junction temperatures as low as possible. The JPL derating guidelines provides margin to the manufacturer's maximum allowed temperature. Additional margin is achieved by limiting the temperature rise from the mounting surface to the junction via good thermal design of the electronics package, since in flight the mounting surface will be held to the allowable flight temperature range.*

4.12.6.2 **Bus electronics design temperature range** - For Type I, bus electronics **shall** be designed to operate within specification over the temperature range of −35°C to +70°C or AFT temperature limits extended by −15°C and +20°C, whichever is more severe. For Type II and Type 0, bus electronics **shall** be designed to operate within specification over the AFT temperature limits extended by −15°C and +20°C.

4.12.6.3 **Payload/Instrument electronics design temperature range (excluding detectors and other instrument-unique hardware)** - For Type I, the payload instrument electronics **shall** be designed to operate within specification over the temperature range of −35°C to +70°C or AFT temperature limits extended by −15°C and +20°C, whichever is more severe. For Type II and Type 0, the payload instrument electronics **shall** be designed to operate within specification over the AFT temperature limits extended by −15°C and +20°C.

4.12.6.4 **Design temperature range for detectors and other instrument-unique hardware** – Detectors and other instrument-unique hardware

shall be designed for allowable flight temperature (AFT) limits extended by −15°C and +20°C.

Rationale: Design margins provide insurance against the unknowns and unexpected events in the mission. Design margins of −15°C/+20°C beyond the AFT ensure the detectors and other instrument-unique hardware are robust and will have predictable performance and graceful degradation over time and in the event of temperature excursions.

***Note:** Detectors and other instrument-unique hardware (e.g., highly stable oscillators) that require a very narrow temperature range for their proper operation may define a separate temperature range for in-specification performance upon agreement with the project.*

4.12.6.5 **Battery design temperature range** – For Li-ion batteries, the hardware **shall** be designed to operate within specification over the AFT temperature limits extended by −10°C and +10°C. For all other battery technologies, the hardware **shall** be designed to operate within specification over the AFT temperature limits extended by −15°C and +20°C.

Rationale: The intent of this requirement is to preserve the life span of the flight batteries as well as mitigate safety concerns during qualification testing. Batteries are not included in the category of bus electronics. Any electronics included in the integrated battery are expected to be compliant with the bus electronics design temperature range.

4.12.7 Power On/Off and Reset (POR) Design Considerations in Electronic Assemblies

4.12.7.1 **POR state** - At prime power turn-on or recovery from a power under-voltage condition, each subsystem **shall** autonomously configure to a unique, unambiguous, safe, system compatible state.

4.12.7.2 **POR visibility** - A POR occurrence **shall** be unambiguously identifiable via telemetry.

4.12.7.3 **Power-on reset circuits** - Reset circuits **shall** be designed to provide control of the electronic circuitry through the transition from the power off state until the circuit is configured for operation, and at power down until the voltage has dropped to a sufficient level to prevent unintended circuit behavior and spurious outputs.

Rationale: Circuit output signals can be undefined and potentially cause damage during voltages outside of the nominal operating range.

Note: *POR signals may need to be provided from external reset circuits to ensure proper reset sequencing during start-up and shutdown transitions.*

4.12.7.4 **Robustness to Primary Power Faults** - Flight Electronic assemblies **shall** (*should* for Type II), be designed to tolerate primary power voltage deviations below the nominal operating voltages for the S/C power bus (e.g., any voltages between 0-to-22 Volts) of indefinite durations, without damage to the assembly and then be capable of full recovery once the power bus is restored.

Note: *Applies as long as environmental collateral damage, resulting from the S/C power bus loss, hasn't damaged the assembly (e.g., temperature excursions outside the limits of the electronic hardware).*

Rationale: Electronic assemblies need to be able to protect themselves from damage due to intermediate voltages on the power bus that may occur during S/C power-bus under-voltage events or during test related scenarios. Collateral damage due to non-power bus related effects, such as temperature excursions outside the qualification temperature limits of the assembly (that may occur if the power bus is lost) are not covered by this DP.

4.12.8 **Hazard Controls**

4.12.8.1 **High voltage activation** - High voltage power supplies **shall** have at least two independent, separate controls to activate/deactivate high voltage to assure that no single fault/command can result in high voltage state, which may result in risk to personnel or hardware, or be a mission safety hazard.

4.12.8.2 **Visibility into state of safety inhibits** - The state of hardware inhibits used to control s/c hazards **shall** be available with and without s/c power on. For example, the state of relays used to safe s/c pyrotechnics is monitored at support equipment.

4.12.9 **Flight Hardware Margins** - See 6.3.8

4.12.10 Verification

4.12.10.1 **Testability** - Electronics systems and circuit boards *should* be designed to allow functional and electrical checkout and in-situ troubleshooting prior to and after integration at the next higher assembly level.

Note: *Typical provisions include test points and test ports that are accessible throughout increasing levels of hardware integration.*

4.12.11 Electro-mechanical

4.12.11.1 **Relays** - The design **shall** be immune to relay contact bounce that is expected in normal operation, and to contact transfer if that may occur when the relays are exposed to the mission shock environment.

Note: *If electrical circuits cannot tolerate these conditions, then some mitigating response is indicated, e.g., the relays may need special mounting provisions to reduce the shock environment, or electrical excitation may need to be applied to "clench" the relay in the required state.*

5.0 *Deleted*

6.0 Managed Margins

6.1 *Deleted*

6.2 Mission Design Resource Margins

6.2.1 Propellant

6.2.1.1 **Propellant margins at key project life cycle milestones** - See 4.7.2 and 6.3.2

6.2.1.2 **Treatment of statistical delta-V estimates** - See 3.2.1

6.3 Flight System Technical Resource Margins

Waivers. Many of the requirements in this section define technical margins required at milestones prior to launch. If the margin for the upcoming milestone does not meet the requirement but mitigation plans are in place to bring the project into compliance by the next milestone, the project reports the non-compliance to institutional stakeholders prior to the review and vets the plan with

the review board at the review. No waiver is required in this case. In some situations, a project may choose to write a waiver in order to reach institutional agreement on an alternate set of margins at milestones.

Quoting margins. Formulas for determining technical margins may vary between organizations. Therefore, it is good practice, when quoting a margin value, to always include the actual formula or information about which formula was used (e.g., “JPL DP9 formula”).

Applicable phases. The technical margins in Section 6.3 are specified for project life-cycle milestones from Phase B entry (Mission Definition Review [MDR]/Project Mission System Review [PMSR]) through launch (margins for Phase E are specified in Section 9.5). Because of the higher variability during early formulation, margins for Pre-Phase A, Mission Concept Review (MCR), and Phase A are not explicitly specified in this Design Principles document. This does not imply that the MDR/PMSR margins are sufficient for these earlier phases. On the contrary, because margin will be consumed during these early formulation activities, just as it is in later phases, margins during Pre-Phase A, MCR, and Phase A still need to be higher than those specified here for MDR/PMSR. Higher margins should be held such that as margin is consumed, the remaining margin at the end of Phase A can credibly be expected to meet the required margin levels at MDR/PMSR. The question of how much higher is currently left to the proposal and study teams and their reviewers.

6.3.1 Alternative Margin Documentation

Type 0 projects **shall** document alternative margins, if different, in an approved Project Plan, in lieu of writing a waiver.

This requirement is applicable to only the following paragraphs: 4.3.3.2, 4.3.3.5, 4.8.2.11, 6.3.2.3, 6.3.3.3, 6.3.3.5, 6.3.5.3, 6.3.6.1, 6.3.6.2, 6.3.8.1, 6.3.9.1, 6.3.10.1, 7.6.4.

6.3.2 System Mass Margins

System mass margins are established and managed throughout the project development in order to manage risk and accommodate mass growth that typically occurs as the project matures.

This section is intended to be generally consistent with the following industry standards and practice: Mass Properties Control for Space Systems, ANSI/AIAA Standard S-120A-2015 and Mass Properties Control for Space Systems, SAWE Recommended Practice No A-3

This section incorporates the key definitions and requirements for management of mass margin from S-120A-2015, with some tailoring for JPL’s mission set --the

"what". More detailed guidance on process and practice for management of mass properties in general can be found in "Recommended Practice for Mass Properties Management on JPL Projects" (based on the SAWE Recommended Practice A-3 above) -- the "how".

In the event of discrepancies, the JPL documents take precedence.

6.3.2.1 System mass margin definitions

See Fig 6.3.2-1 for a graphical summary of the relationships among the key definitions.

Basic Mass - The current mass of dry hardware based on an assessment of the most recent baseline design.

Note 1: *The design assessment includes the estimated, calculated, or measured mass and includes an estimate for undefined design details like cables, multi-layer insulation, and adhesives.*

Note 2: *Basic mass includes a nominal estimate of any balance or ballast mass(es) for CM or inertia control of the fueled flight system.*

Note 3: *The Mass Growth Allowances (MGA) and uncertainties are not included in the basic mass.*

Note 4: *Pending and potential changes are not included in the basic mass.*

Dry Mass - The mass of a flight system, or components thereof, not including usable propellants.

Note: *Inert fluids or gases (e.g., pressurization gases, hydraulic fluids, thermal working fluids) and the unusable portion of propellants are considered part of dry mass.*

Mass Growth Allowance (MGA) - The predicted change to the basic mass of an item based on an assessment of the hardware category, design maturity, and fabrication status.

Note 1: *The MGA is applied at the lowest design detail level reported in the mass properties database.*

Note 2: *Mass growth allowance varies as a function of hardware and its design maturity. Depletion of the MGA follows the design*

process; as the design and analyses of the hardware matures, the MGA depletes to reflect increased confidence in the predicted final mass. For guidance on selection of MGA values, see "Recommended Practice for Mass Properties Management on JPL Projects."

Predicted Mass - The sum of the basic mass and the MGA; intended to estimate the final mass at system delivery or operation.

Allowable Mass - The mass limit against which a mass margin is calculated.

Note 1: *The allowable mass is a derived requirement set early in the program/project and is intended to remain constant until there is a change in requirements. At the flight system level, an example of a change in requirements would be a new launch vehicle, launch date or trajectory.*

Note 2: *An allowable mass may refer to (or be stated in terms of) a dry mass or a wet mass, so long as the intended content is unambiguous.*

Note 3: *At the flight system level, this mass limit usually results from bounds on the launch vehicle's capability. Other examples of an allowable mass include a contractor Not-to-Exceed (NTE) mass limit or a mass allocation to a design organization.*

Mass Reserve - The mass allowance defined and retained by management at a higher level for potential scope changes or any other unforeseen mass impacts (e.g., new discoveries such as new environmental requirements).

Note 1: *The launch service provider may also hold back mass reserves, providing a lower performance commitment (i.e., allowable mass at launch) to the project than the nominal launch vehicle capability. This "reserve" is not under the control of the project, and should not be considered part of the project's allowable mass.*

Note 2: *When allocating allowable masses across multiple flight system segments, stages, or subsystems based on a higher-level mass allowance, the mass reserve is by definition the difference between the higher-level allowable mass and the sum of the next lower-level allowable masses. The mass reserve from such an allocation may be zero, but never negative.*

Mass Margin = Allowable Mass – Predicted Mass. The mass available for in-scope changes.

% Mass Margin = ((Allowable Mass – Predicted Mass)/Basic Mass) x 100

% MGA = (MGA/Basic Mass) x 100

% (MGA + Mass Margin) = ((Allowable Mass – Basic Mass)/Basic Mass) x 100

Wet Mass - The mass of a flight system including dry mass and usable propellants.

Note: *The launch service provider's "performance commitment" (also known as the "payload allocation") represents the mass limit on the wet mass. The predicted flight system wet mass is compared to this performance commitment to obtain the wet mass margin.*

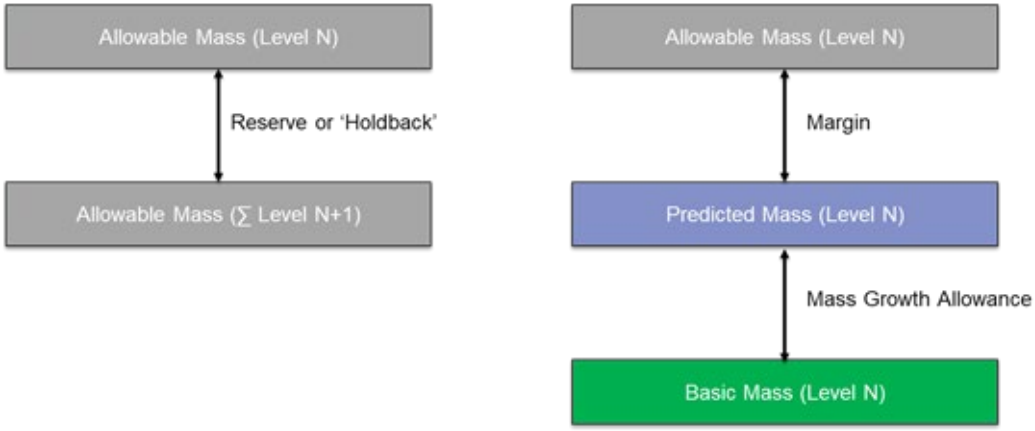

Figure 6.3.2-1 **Fundamental Relationships Among Flight System Allowable, Predicted, and Basic Masses**

6.3.2.2 ***Deleted***

6.3.2.3 **Flight System % Mass Margin Requirements at Key Project Life Cycle Milestones** - Flight System % Mass Margin at Key Project Life Cycle Milestones **shall** (*should* for Type II) be greater than or equal to those shown in Table 6.3.2-1.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.2-1 System Dry Mass Margin at Key Life Cycle Milestones

Key Project Life Cycle Milestones				
MDR/PMSR	PDR	CDR	SIR	Launch
23%	12%	5%	2%	0%

Rationale: During development, projects use mass margin both to accommodate expected growth as the design matures, and also to cover problem resolution and other design changes. An effective process for estimating expected growth will inform the project as to the margin needed for growth (see Recommended Practice for Mass Properties Management on JPL Projects). By contrast, this Design Rule specifies the level of margin projects must keep over and above expected growth, i.e., margin which is not already encumbered by future maturation. Together with reasonable assumptions on overall MGA at each life cycle milestone, they represent a roughly equivalent level of % margin as was required by DP versions prior to DP9, which were rounded to multiples of 5%.

Note 1: *As used in this requirement:*

- *Flight System Allowable Mass is the dry mass fraction of the allowable flight system wet launch mass. It includes any reserves held by the project. It does not include reserves held external to the project (for example, by the launch service provider);*
- *Flight System Predicted Mass is the sum of the predicted masses of the spacecraft and payload;*
- *Flight System Basic Mass is the sum of the basic masses of the spacecraft and payload.*

Note 2: *These margin requirements apply only at the Flight System level. Allowable masses below the Flight System level (e.g., Spacecraft, Payload, Subsystems) are set by projects and may have different margins. (Exception: on projects where JPL deliverable is an instrument to fly on a non-JPL spacecraft, these margin requirements apply at the instrument project level, relative to the allowable mass as specified by the integrator.)*

Note 3: *While these limits are representative of past experience, they are neither a guarantee of all the resources a project will need to handle its development issues, nor a statement of certainty that projects always consume the full margins in addressing their development issues. Limits are established in order to create the dialog for the risks being taken should a project imagine the past experience does not apply in their instance, for example in the case of "build-to-print" missions.*

6.3.2.4 ***Deleted***

6.3.2.5 **Propellant load sizing** - The usable propellant load **shall** be sized to provide the baseline mission required delta velocity for the flight system allowable mass including any reserves held by the project.

Rationale: Assuming the flight system dry mass grows all the way to the dry mass fraction of the allowable flight system wet launch mass, the flight system will need to carry sufficient propellant to push that dry mass through the baseline mission delta velocity.

Note: *This requirement applies at the flight system level. Propellant load sizing for staged vehicles may use different assumptions.*

6.3.3 System Power/Energy Margins

System power and energy margins are established and managed throughout the project development in order to manage risk and accommodate growth that typically occurs as the project matures. Growth in this context can include increases in power consumption, increases in conversion and transmission losses, and decreases in power generation and energy storage capability.

The management of power and energy during development is a multifaceted and cross-cutting endeavor. It involves heavy interdependence between mission scenarios, power, thermal, and harness designs. Consumption, production, power handling, and storage must all be considered. Several types of consumption need to be accounted for, including steady state and peak usage. Values for the key parameters may change throughout the mission, most often through degradation from environmental factors such as radiation, requiring explicit treatment of beginning-of-life and end-of-life cases.

This section provides guidance on management of three key types of margin: system power, system energy, and battery state of charge. Which margins are most useful, and which scenarios or cases to analyze, depend strongly on the specific mission characteristics, operational scenarios, and flight system technologies. Projects will determine which cases drive design and use the

appropriate margin metrics to manage the design. The requirements in this DP apply to the power/energy characteristics determined to be driving by the project.

In the case of missions utilizing electric propulsion, power is a coupled resource with mass and thrust time. As such, these resources can be rebalanced in a process that will be described in external guidance.

This section is intended to be generally consistent with the following industry standards and practice, with some tailoring: Electrical Power Systems for Unmanned Spacecraft, AIAA Standard S-122-2007. In the event of discrepancies, the JPL document takes precedence.

6.3.3.1 **System power margin definitions** – **for non-electric propulsion missions** – See Figure 6.3.3-1 for a graphical summary of the relationships among the key definitions.

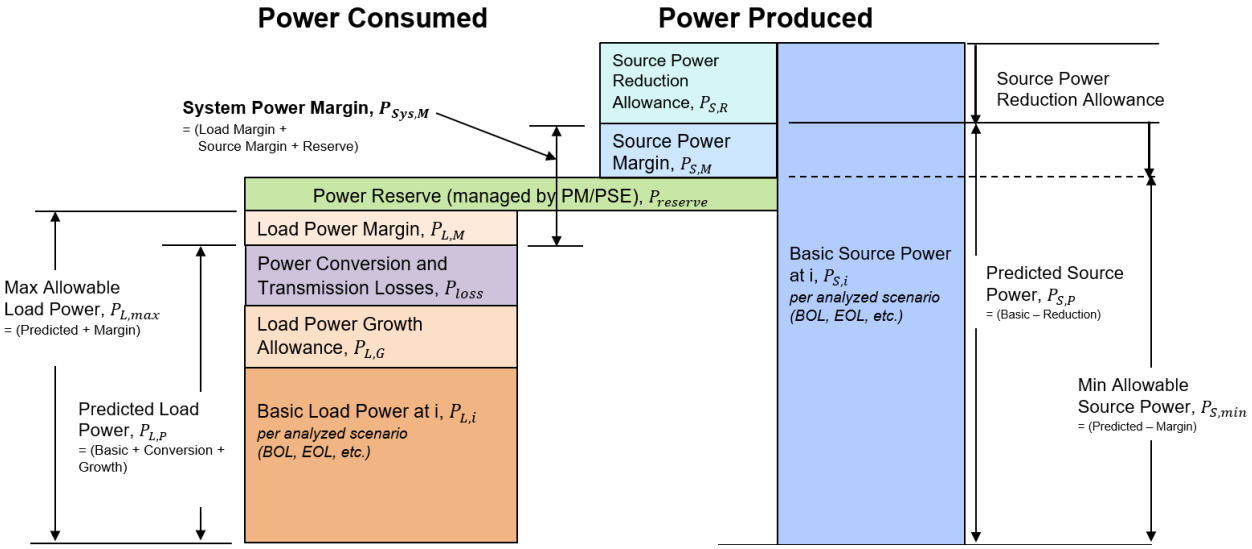

Figure 6.3.3-1 **Power Margin – Summary of Terms**

Basic Load Power at i ($P_{L,i}$) - $P_{L,i}$ is the current estimate of power consumption, taking into account everything known but exclusive of the growth that likely will occur as the design matures. Estimated for each relevant scenario, for example at Beginning of Life (BOL), End of Life (EOL), and at any points in between, such as EDL, where power margin may be limited. The subscript i can be interpreted as a mode, an event, or an instant in time, associated with an average power, depending on the scenario being analyzed.

***Note 1**: Power consumption here is intended to include steady state or average rather than transient or peak power loads. Steady state is usually taken to mean "constant over periods greater than 50 - 100 ms," whereas a shorter duration is generally*

taken to be a transient, although the exact limit may vary from application to application. Steady state is distinguished from peak in that peak power is generally a worst-case estimate, used for sizing current carrying capacity, battery discharge limits, etc. As a worst-case estimate, it would not have an associated Load Power Growth Allowance or Predicted Load Power value, and the required margins in this section would not apply.

Note 2: *Load includes resistive losses in passive components, such as wires within the device.*

Note 3: *Load includes power required for battery charging. This will vary depending on the scenario.*

Note 4: *Load estimates need to account for environmental characteristics, such as temperature.*

Note 5: *$P_{L,i}$ at BOL normally corresponds to the launch scenario. This should not include load changes resulting from EOL degradation factors (e.g., lifetime, radiation, material and surface properties, degradation from thermal cycling) but may include any degradation during storage prior to launch.*

Note 6: *$P_{L,i}$ at EOL normally corresponds to a scenario of required activities occurring at the end of mission, for example deorbit. This should include load changes resulting from EOL degradation factors (e.g., lifetime, radiation, material and surface properties, degradation from thermal cycling).*

Load Power Growth Allowance ($P_{L,G}$ or % $P_{L,G}$) - $P_{L,G}$ is the predicted change to the Basic Load Power value based on an assessment of the design maturity, historical trends, and an estimate of the in-scope design changes that may still occur throughout the life cycle (known unknowns). This value may be expressed either as a percentage with respect to $P_{L,i}$ or as a quantity with units (e.g., 5 W).

$$\%P_{L,G}=P_{L,G}/P_{L,i} \times 100$$

Note 1: *Load Power Growth Allowance is applied at the lowest design detail level reported in the Powered Equipment List (PEL).*

Note 2: *Growth should not include degradation over life –that is accounted for in EOL Basic Load Power.*

Note 3: *In-scope design changes could include, for example, planned future down-select of specific parts or interface technologies,*

or current uncertainty as to power conversion efficiency. These uncertainties should be accounted for in % $P_{L,G}$. Out-of-scope changes—for example, those involving potential requirements changes—should be tracked as threats to be accommodated from margin or reserve.

Power Conversion and Transmission Losses (P_{loss}) - P_{loss} is losses incurred during the conversion or regulation of power, and losses incurred due to resistive losses in cabling.

Predicted Load Power ($P_{L,P}$) - $P_{L,P}$ is the sum of Basic Load Power, Power Conversion and Transmission Losses, and Load Power Growth Allowance.

$$P_{L,P} = P_{L,I} + P_{loss} + P_{L,G}$$

Maximum Allowable Load Power ($P_{L,max}$) - $P_{L,max}$ is the required not-to-exceed value for steady state Load.

Note 1: *At the flight system (or instrument project) level, Maximum Allowable Load Power is the Minimum Allowable Source Power (in the absence of reserve). Lower levels of assembly will be allocated a subset of this capability.*

Load Power Margin ($P_{L,M}$) - $P_{L,M}$ is the difference between Maximum Allowable Load Power and Predicted Load Power.

$$P_{L,M} = P_{L,max} - P_{L,P}$$

Note 1: *In addition to EOL values, which are often used for system sizing early in formulation, other points in the mission timeline may be used where appropriate (e.g., orbit insertion). Ensure that all values used are self-consistent (e.g., all values are at BOL, EOL, or whatever other point is being defined).*

Basic Source Power at *i* ($P_{S,i}$) - $P_{S,i}$ is the current estimate of power production, taking into account everything known but exclusive of the reductions that likely will occur as the design matures. $P_{S,i}$ is estimated for each relevant scenario, for example at BOL, EOL, and any points in between, such as EDL, where power margin may be limited.

Note 1: *Source estimates need to account for environmental conditions such as temperature.*

Note 2: $P_{S,i}$ *at BOL normally corresponds to the launch scenario. This should not include EOL degradation factors (e.g., lifetime,*

radiation, material and surface properties, degradation from thermal cycling) but may include any degradation during storage prior to launch.

Note 3: $P_{S,i}$ *at EOL normally corresponds to a scenario of required activities occurring at the end of mission, for example deorbit. This should include EOL parts degradation factors (e.g., lifetime, radiation, material and surface properties, degradation from thermal cycling). If any of the degradation factors is a significant contributor (~>10%) to* $P_{S,i}$ *it should be identified in the Basis of Estimate.*

Source Power Reduction Allowance ($P_{S,R}$ or $\%P_{S,R}$) - $P_{S,R}$ is the predicted change to the Basic Source Power value based on an assessment of the design maturity, historical trends, and an estimate of the in-scope design changes that may still occur throughout the life cycle (known unknowns). This value may be expressed either as a percentage with respect to $P_{S,i}$, or as a quantity with units (e.g., 5 W).

Note 1: *The* $P_{S,R}$ *is applied at the lowest design detail level reported in the PEL.*

Note 2: *Decreases should not include degradation over life—those are accounted for in EOL Basic Source Power.*

Note 3: *In-scope design changes could include, for example, changes in assumed photovoltaic cell packing factor or cover glass thickness, the potential addition of battery capacity as scenarios mature, or uncertainty on performance and degradation in radiation environment. These uncertainties should be accounted for in* $\%P_{S,R}$*. Out-of-scope changes involving, for example, potential requirements changes, should be tracked as threats to be accommodated from margin or reserve.*

Predicted Source Power ($P_{S,P}$) - $P_{S,P}$ is the difference between Basic Source Power and Source Power Reduction Allowance.

$$P_{S,P} = P_{S,i} - P_{S,R}$$

Minimum Allowable Source Power ($P_{S,min}$) - $P_{S,min}$ is the required minimum value for steady state Source Power capability. Minimum Allowable Source Power is the reference for establishing the margin.

Source Power Margin ($P_{S,M}$) - $P_{S,M}$ is the difference between Predicted Source Power and Minimum Allowable Source Power.

$$P_{S,M} = P_{S,P} - P_{S,min}$$

Note 1: *In addition to EOL values, which are often used for system sizing early in formulation, other points in the mission timeline may be used where appropriate (e.g., orbit insertion). Ensure that all values used are self-consistent (e.g., all values are at BOL, EOL, or whatever other point is being defined).*

Power Reserve ($P_{reserve}$) - $P_{reserve}$ is the power allowance, if any, defined and retained by management at a higher level for potential scope changes or any other unforeseen power impacts, in either source or load.

System Power Margin ($P_{Sys,M}$) - $P_{Sys,M}$ is the sum of Load Power Margin, Source Power Margin, and Power Reserve. It is a measure of margin available for growth of loads, by assessing source, load, and storage over any desired scenario.

$$P_{Sys,M} = P_{L,M} + P_{S,M} + P_{reserve}$$

$$P_{Sys,M} = P_{S,P} - P_{L,P}$$

Note 1: *This metric is applicable to the following:*

- *Systems with power source and storage (e.g., Europa Clipper). Both power and energy need to be analyzed.*
- *Systems with power source only and no energy storage (e.g., Cassini). Calculate margin on a pure power basis.*
- *Storage-only missions (primary or thermal battery). Use this to ensure power draw does not exceed battery rated capability.*

Note 2: *This margin explicitly excludes the growth allowances. It represents margin unencumbered by expected growth.*

Note 3: *The specific scenario is as defined by the project, from a determination of the driving design case(s). All values used in the computation should be consistent with respect to the scenario being analyzed.*

Note 4: *The common methodology for determining system power margin is by inflating the predicted load power to the limits of the system (minimum state of charge, maximum capability, etc.).*

% System Power Margin (% $P_{Sys,M}$) - % $P_{Sys,M}$ is $P_{Sys,M}$ expressed as a percentage of Basic Load Power.

$$\% P_{Sys,M} = P_{Sys,M}/P_{L,i} \times 100$$

Rationale 1: Load (rather than Capability) is used in the denominator, to be consistent with the standard for power margin (AIAA S-122-2007), which uses load.

Rationale 2: Basic (rather than Predicted or Allowable) Load Power is used in the denominator in order to

- *allow simple summing with % Growth Allowance, and*
- *be consistent with the definition of % System Mass Margin in Section 6.3.2 and the ANSI/AIAA Standard S-120A-2015, both of which use Basic mass. Unfortunately, this causes an inconsistency with the power standard AIAA S-122-2007, which uses Predicted Load in the denominator (termed Contingent Load Power) rather than Basic Load. This inconsistency is accepted in order for these DPs to be internally consistent.*

6.3.3.2 System energy margin definitions – for non-electric propulsion missions

See Figure 6.3.3-2 for a graphical summary of the relationships among the key definitions.

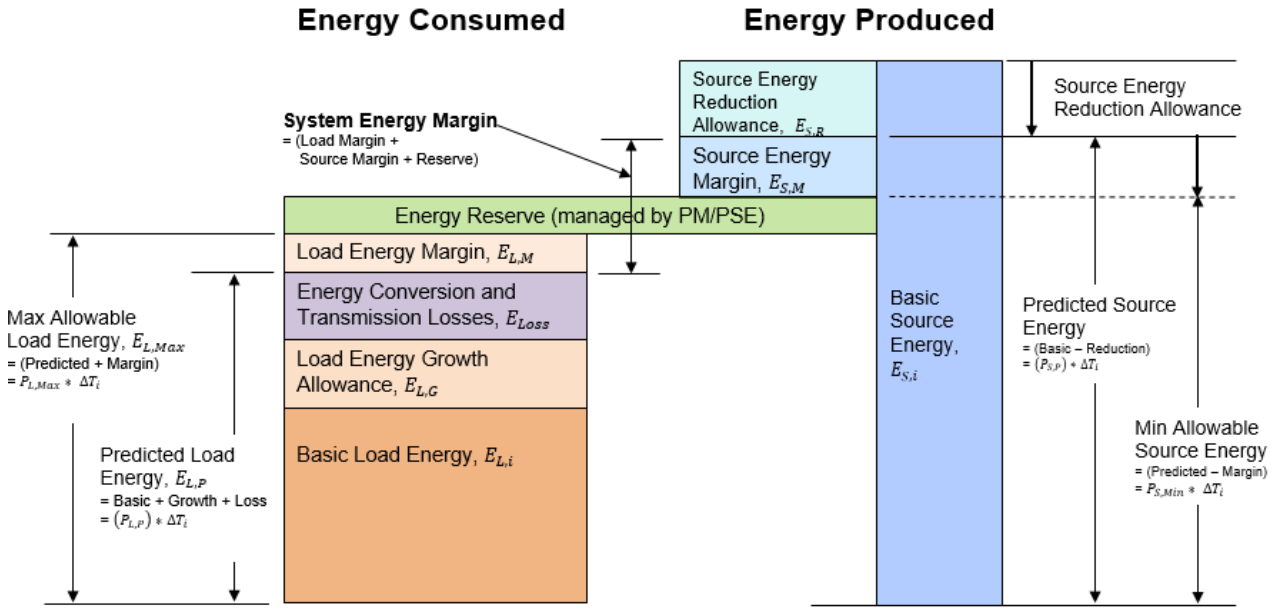

Figure 6.3.3-2 **Energy Margin – Summary of Terms**

Basic Duration of the energy analysis Epoch *i* (*ΔTi*) - ΔT_i is the current estimate of the duration, taking into account everything known but exclusive of growth that may occur as the mission design matures.

Note 1: *Epoch i is defined generally as a discrete time slice, which could be an activity, event, or phase, depending on the scenario being analyzed. The power load during Epoch i can be a constant or an average. Complex activities such as EDL may be divided into many discrete time slices, each with their own constant or average load power, to compute energy as an integral, where ΔT_i forms the limits of integration, e.g.,*

$$\int_{t}^{t+\Delta T} P(t) \times dt.$$

Note 2: *Uncertainty/growth in the Epoch Duration estimate needs to be accounted for in order to manage uncertainty/growth in the energy estimate. This may be done in one of several ways, with the choice being driven by the specific characteristics of each project. Hence, the DPs do not prescribe a particular method.*

Basic Load Energy ($E_{L,i}$) - $E_{L,i}$ is the Basic Load Power multiplied by the Basic Duration.

$$E_{L,i} = P_{L,I} \times \Delta T_i$$

Example of basic load energy at BOL: $E_{L,BOL} = P_{L,BOL} \times \Delta T_{BOL}$

Example of basic load energy at EOL: $E_{L,EOL} = P_{L,EOL} \times \Delta T_{EOL}$

Note 1: *In systems with energy storage such as a battery, Load Energy includes power required for battery charging (included in the estimate of Basic Load Power).*

Note 2: *When power is constant or can be analyzed as an average, the expression as a product (above) can be used; in cases where power varies significantly over time, an integral expression is indicated, i.e.,*

$$\int_{t}^{t+\Delta T} P(t) \times dt$$

Load Energy Growth Allowance ($E_{L,G}$) - $E_{L,G}$ is the Load Power Growth Allowance multiplied by the Basic Duration.

$$E_{L,G} = P_{L,G} \times \Delta T_i$$

Predicted Load Energy ($E_{L,P}$) - $E_{L,P}$ is the Predicted Load Power multiplied by the Basic Duration.

$$E_{L,P} = P_{L,P} \times \Delta T_i$$

Maximum Allowable Load Energy ($E_{L,max}$) - $E_{L,max}$ is the Maximum Allowable Load Power multiplied by the Basic Duration.

$$E_{L,max} = P_{L,max} \times \Delta T_i$$

Load Energy Margin ($E_{L,M}$) - $E_{L,M}$ is the difference between Maximum Allowable Load Energy and Predicted Load Energy.

$$E_{L,M} = E_{L,max} - E_{L,P}$$

Basic Source Energy ($E_{S,i}$) - $E_{S,i}$ is the Basic Source Power multiplied by the Basic Duration.

$$E_{S,i} = P_{S,I} \times \Delta T_i$$

Example of basic source margin at BOL: $E_{S,BOL} = P_{S,BOL} \times \Delta T_{BOL}$

Example of basic source margin at EOL: $E_{S,EOL} = P_{S,EOL} \times \Delta T_{EOL}$

Note 1: *In systems with energy storage such as a battery, Source Energy includes usable energy from these storage devices. This will vary depending on the scenario.*

Note 2: *When power is constant or can be analyzed as an average, the expression as a product (above) can be used; in cases where power varies significantly over time, an integral expression is indicated, i.e.,*

$$\int_{t}^{t+\Delta T} P(t) \times dt$$

Source Energy Reduction Allowance ($E_{S,R}$) - $E_{S,R}$ is the Source Power Reduction Allowance multiplied by the Basic Duration.

$$E_{S,R} = P_{S,R} \times \Delta T_i$$

Predicted Source Energy ($E_{S,P}$) - $E_{S,P}$ is the Predicted Source Power multiplied by the Basic Duration.

$$E_{S,P} = P_{S,P} \times \Delta T_i$$

Minimum Allowable Source Energy ($E_{S,min}$) - $E_{S,\,min}$ is the Minimum Allowable Source Power multiplied by the Basic Duration.

$$E_{S,min} = P_{S,min} \times \Delta T_i$$

Source Energy Margin ($E_{S,M}$) - $E_{S,M}$ is the difference between Predicted Source Energy and Minimum Allowable Source Energy.

$$E_{S,M} = E_{S,P} - E_{S,min}$$

Energy Reserve ($E_{reserve}$) - $E_{reserve}$ is the Energy allowance, if any, defined and retained by management at a higher level for potential scope changes or any other unforeseen Energy impacts, in either source or load.

Energy Margin ($E_{Sys,M}$) - $E_{Sys,M}$ is the difference between Predicted Source Energy and Predicted Load Energy. It is a measure of net energy available over a defined epoch.

$$E_{Sys,M} = E_{S,P} - E_{L,P}$$

Note 1: *System energy management is indicated for modes of operation in which the spacecraft system's demands exceed the power available. For cyclical uses, periodicity is*

determined by the steady state condition where a balance exists between energy usage and restoration.

Note 2: *This metric is useful for providing a simple epoch-level accounting of net energy available (e.g., maintaining positive energy margin on all orbits has the benefit of precluding coupling from one orbit to the next). The main limitation is that it is not perceptive to timing of source or load events, where high loads over short periods could cause undervoltage or violate minimum state of charge requirements, but energy margin over the epoch may still be positive (e.g., as on Clipper, where long relatively quiescent orbits are punctuated by brief periods of intense activity around Europa flybys). Additionally, caution is indicated over long epochs, when a large energy margin may in fact be only a small margin when computed as a percentage. The % Energy Margin should be used in these cases. This margin is applicable to the following:*

- *Systems with power source and storage (e.g., Clipper)*
- *Systems with storage-only missions (primary or thermal battery). The defined epoch is usually the full mission.*

This margin is not applicable for missions with power source only and no storage (e.g., Cassini).

Note 3: *This margin explicitly excludes the growth/reduction allowances. It represents unencumbered margin for true unknowns.*

Note 4: *The specific scenario is as defined by the project from a determination of the driving design case(s).*

% Energy Margin (%$E_{Sys,M}$) - %$E_{Sys,M}$ is the Energy Margin expressed as a percentage of the Basic Load Energy.

$$\%E_{Sys,M} = E_{Sys,M} / E_{L,i} \times 100$$

Rationale 1: Load (rather than Capability) is used in the denominator, to be consistent with the standard for power margin (AIAA S-122-2007), which uses load.

Rationale 2: Basic (rather than Predicted or Allowable) Load Energy is used in the denominator in order to

- *allow simple summing with % Growth Allowance, and*

- *be consistent with the definition of % System Mass Margin in Section 6.3.2 and the ANSI/AIAA Standard S-120A-2015, both of which use Basic mass. Unfortunately, this causes an inconsistency with the power standard AIAA S-122-2007, which uses Predicted Load in the denominator (termed Contingent Load Power) rather than Basic Load. This inconsistency is accepted in order for these DPs to be internally consistent.*

6.3.3.3 System % power/energy margins at key project life cycle milestones

System % power/energy margins at key project life cycle milestones applying to mission-critical and mission-enabling modes, including cruise, science operations, and safing modes, **shall** (*should* for Type II) meet or exceed those shown in Table 6.3.3-1.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.3-1 System % Power/Energy Margin at Key Life Cycle Milestones

Key Project Life Cycle Milestones				
MDR/PMSR	**PDR**	**CDR**	**SIR**	**Launch**
25%	15%	12%	10%	10%

Rationale: During development, projects use power/energy margin both to accommodate expected growth as the design matures and to cover problem resolution and other design changes. This design rule specifies the level of margin projects must keep over and above expected growth, i.e., margin which is not already encumbered by future maturation. An effective process for estimating expected growth is important to ensure that the unencumbered margin is actually unencumbered. Assumptions on aggregated growth allowances at each life cycle milestone, together with the required margins in Table 6.3.3-1, represent a total level of % margin similar to that required by pre-DP10 versions.

Note 1: *These margin requirements apply only at the flight system level, or in the case of instrument projects, at the instrument*

project level. Maximum Allowable Power Consumption or Minimum Allowable Power Production at lower levels (e.g., spacecraft, payload, subsystems) are set by projects and may have different margins.

Note 2: *These power margin requirements do not apply to power use that is uniquely associated with electric propulsion systems. Margins appropriate to electric propulsion–unique power use need to accommodate spacecraft uncertainties (e.g., solar array output, power conditioning efficiency) and take into account flexibility to thrusting (e.g., thrust levels, coast periods) inherent in the trajectory design. Guidance for project-specific application of the approaches used on recent past projects is available from subject-matter experts.*

Note 3: *While these limits are representative of past experience, they are neither a guarantee of all the resources a project will need to handle its development issues, nor a statement of certainty that projects always consume the full margins in addressing their development issues. Limits are established in order to create the dialog for the risks being taken should a project imagine the past experience does not apply in their instance, for example in the case of "build-to-print" missions.*

6.3.3.4 Battery State of Charge Margin Definitions

See Section 4.3.3.6 for definitions of battery DOD and capacity, and design rules on minimum DOD based on battery chemistry and charge/discharge cycles. Section 6.3.3.4 builds on that section to provide additional definitions and design rules on state of charge margin as a component of system power/energy margin.

Battery Capacity (E_C) - E_C is a measure of the charge stored by the battery (typically in Amp-hr) but may also be expressed as a measure of energy delivered by the battery (E_B) under the specified discharge conditions (typically in Watt-hour). For the purpose of State of Charge Margin management, the remainder of this section uses the charge-based definitions.

See Section 4.3.3.6.1 for definition and usage. (Note that 4.3.3.6.1.b currently requires battery capacity removed during discharge to be based on the CBE plus uncertainty of loads. Starting with DP10, this is interpreted as "Predicted Loads.")

Charge/Discharge Rate - The Charge/Discharge Rate is the amount of charge added to/subtracted from the battery per unit time.

Discharge rate is defined as the steady current in amperes (A) that can be taken from a battery of defined capacity (Ah) over a defined period (h).

The constant charge or discharge current for a battery is defined as C/*n*, or C-rate. C is the cell-level nameplate (or rated) capacity in ampere-hours (per vendor's criteria), and *n* is any value for elapsed time measured in hours. For example, a discharge current of C/2 for a 20 Ah–rated cell is a discharge current of 10 A.

% State of Charge (SOC_C) based on battery capacity - SOC_C is the capacity remaining in battery divided by total capacity of battery defined in Amp-hours.

$$SOC_C = E_{C(remaining)} / E_{C(available)} \times 100\%$$

Or (100%−DOD) with DOD as defined in Section 4.3.3.6.1.

See Section 4.3.3.6.1.c for information on how battery capacity is influenced by age, temperature, and rate of discharge.

Minimum % State of Charge (SOC_{min}) - SOC_{min} is the minimum state of charge realized over a defined mission event, both nominal and off-nominal.

Estimates of SOC_{min} for off-nominal mission events need to account for battery capacity used for fault responses (e.g., establishing safe mode, recovering from system undervoltage). Sufficient capacity must be assured to enable completion of these responses.

Minimum Allowed % State of Charge ($SOC_{min,allowed}$) - $SOC_{min,allowed}$ is the minimum state of charge allowed in the battery at any point during the mission.

Note: *Section 4.3.3.6 specifies maximum allowed DODs per chemistry and cycles. In addition, the project may impose lower DOD (higher state of charge) limits to provide capacity for responding to anomalous situations.*

State of Charge Margin (SOC_M) - SOC_M is the difference between the minimum battery state of charge during a mission scenario and the minimum allowed battery state of charge. It is a measure of margin against a project-defined minimum safe state of charge over a defined epoch.

$$SOC_M = SOC_{min} - SOC_{min,allowed}$$

Note: *This metric is useful for evaluating state of charge across a specific time period and is a key metric for battery sizing. It is also an important factor in operations to prevent undervoltages (i.e., the need to account for discharge rate effects on instantaneous state-of-charge measurements in order to prevent inadvertent undervoltages). A key limitation is its insensitivity to power when the system is power positive (e.g., outside of a stressing scenario such as flyby or EDL). It is applicable to the following:*

- *Systems with power source and storage (e.g., Clipper)*
- *Systems with storage-only missions (primary or thermal battery). The defined epoch is usually the full mission*

It is not applicable for missions with power source only and no storage (e.g., Cassini).

6.3.3.5 State of Charge Margins

For systems with batteries, margin above Minimum Allowable State of Charge **shall** (*should* for Type II) meet or exceed the values shown in Table 6.3.3-2.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.3-2 Battery State of Charge Margins

Milestone	Before loads and durations are measured and battery characterized	After loads and durations are measured and battery characterized
% State of Charge Margin	10%	5%

Note 1: *Use Predicted Loads as required by 4.3.3.6.1.b (in DP9, they are still called "CBE plus uncertainty of loads").*

Note 2: *The values in Table 6.3.3-2 are intended for missions with less than 5000 battery cycles per design rule 4.3.3.6.3. For missions with more than 5000 battery cycles, the allowable cyclic DOD is less and the project may establish lower margins accordingly.*

Note 3: *This margin is applicable to the following:*

- *Systems with power source and storage (e.g., Clipper)*
- *Systems with storage-only missions (primary and thermal battery). The defined epoch is usually the full mission.*

This margin is not applicable for missions with power source only and no storage (e.g., Cassini).

6.3.4 ***Deleted***

6.3.5 **Flight Software Margins**

6.3.5.1 **Flight software margins definitions** - The below definitions are used for determining system flight software margins.

Margin = Capability - Current Best Estimate (CBE)

% Margin = 100% * (Margin/Capability)

Note: *Capability is the total capability of the system. If the capability degrades with mission duration, the Capability must reflect the worst-case condition.*

Note: *CBE is the best estimate taking into account everything known, but exclusive of the growth that likely will occur based on maturity.*

6.3.5.2 **System flight software margins** - System flight software margins accommodate expected growth during development. System flight software margins exist at launch to facilitate flight operations, and to allow for post-launch initiated changes with associated impacts on resource usage.

Note: *System flight software margin management is indicated for constrained resources, e.g., computing capacity, memory, throughput, bus bandwidth, etc.*

6.3.5.3 **System flight software margins at key project life cycle milestones** - System flight software margins **shall** (*should* for Type II) be per Table 6.3.5-1.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.5-1 System Flight Software Margins at Key Life Cycle Milestones

Key Life Cycle Milestones				
	Computer Selection	**PDR**	**CDR**	**Launch**
Margins	75%	60%	No specification	20%

6.3.6 Power/Pyrotechnic System Margins

6.3.6.1 **Power distribution circuit margin at key life cycle milestones** - At implementation phase start (Phase C/D), there **shall** (*should* for Type II) be 30% margin on power switch and circuit count, including cabling and connector pins.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Rationale: To accommodate late identified needs (e.g., additional electrical heater(s) for temperature control purposes) with minimum cost and schedule impact.

6.3.6.2 **Pyrotechnic circuit margin at key lifecycle milestones** - At the start of implementation phase, (Phase C/D), there **shall** (*should* for Type II) be 30% margin on pyro firing circuits, including cabling and connector pins.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Rationale: To accommodate late identified needs with minimum cost and schedule impact.

6.3.7 Telecommunications System Margins

6.3.7.1 **Deep space data and tracking link margins at key project life cycle milestones** -

a. At the end of phase A, the design value derived from the current best estimates of the link parameters **shall** exceed the required value by at least 3 db.

b. At the end of phase B, the expected value, derived from a statistical treatment of the parameters and uncertainties, **shall** exceed the

required value by a project-selected multiple of the standard deviation yielding the desired probability of success.

Note: *For command links, 3-sigma below the nominal performance is typically sufficient to meet threshold performance described in 4.5.1.1.*

6.3.8 Flight Electronics Hardware Margins

6.3.8.1 **Flight electronic hardware margins at key life cycle milestones** - Flight electronics development **shall** observe the Table 6.3.8-1 experience-based margins at key development milestones.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.8-1 Flight Electronic Hardware Margins at Key Life Cycle Milestones

Resource	Subsystem PDR	Subsystem CDR	Delivery
PWB area	30%	20%	10%
Connector pin-outs	30%	10%	5%
FPGA gates	40%	20%	10%

6.3.8.2 **Flight electronic hardware margin definition** - The below margin definition applies to all flight electronics hardware resources.

% Margin = 100% * {Unused resource/CBE}

where CBE is the best estimate of the resource use at the key life cycle milestone.

6.3.9 S/C Mechanisms Functional Margins

6.3.9.1 **S/C mechanisms functional margins at key life cycle milestones** - S/C mechanisms design **shall** observe the Table 6.3.9-1 margins at key development milestones.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.9-1 Mechanism Force/Torque Margins at Key Development Milestones

Parameter	Conceptual Design Review	Mechanism PDR	Mechanism CDR	Qualification/ Acceptance Test
Static Torque or Force	175%	150%	125%	100%

Note: *Margins are based on combining worst-case conditions. For cases where high confidence does not exist in the determination of the worst case load or driving capability, a margin considerably higher than that indicated above may be appropriate.*

Rationale: To avoid operational problems and to account for uncertainties.

6.3.9.2 **S/C mechanisms functional margin definitions** - See Section 4.2.3

6.3.10 Energy Margins for Cryogenic Systems

6.3.10.1 **Cryogenic systems margins at key life cycle milestones** - The design of cryogenic systems operating below -70°C **shall** have excess capacity at key development milestones as specified in the Table 6.3.10-1.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 6.3.10-1 Cryogenic System Margins at Key Development Milestones

Parameter	Conceptual Design Review	PDR	CDR	Qualification/ Acceptance Test
Total Cryogenic Load	50%	45%	35%	25%

Note: *Margins apply to both passive and active thermal systems.*

Rationale: Provides design robustness for cryogenic systems below -70 degrees C. Margins are protection for uncertainties and modeling errors on a cryogenic system with a large thermal sensitivity.

6.3.10.2 **Cryogenic systems margin definitions** - The below margin definition applies to cryogenic systems.

Margin = 100% * {[System capacity/CBE heat load] - 1}

Note: *The total cryogenic CBE heat load includes both the active and parasitic heat load components.*

7.0 Flight Scenario Design

7.1 General

7.1.1 **Operation Consistent with Flight Rules** - Flight sequences **shall** operate the spacecraft consistent with flight rules provided by the developers and within environments and functional regimes experienced during development testing.

7.1.2 **Critical Event Telemetry Monitoring** – Mission-critical event and deployment data **shall** (*should* for Type II and Type 0) be available via real-time telemetry.

Rationale: Real time critical event telemetry is needed to monitor that the event occurs as planned, or if not, to determine why not.

Note: *A low cost, moderate reliability transmitter is a possible solution for the lack of real time telemetry at spacecraft separation from the launch vehicle.*

7.1.3 **Ground-in-the-loop Commanding** – No “ground-in-the-loop” commanding **shall** be required after initiation, for mission time-critical operations to be successful.

Note: *The default condition for initiation of time-critical entry, descent and landing depends on the target as follows:*

a. If targeted to Earth, the default is to not initiate the time-critical sequence that results in return to Earth unless the s/c is in receipt of a ground-originated "go" command, and

b. If targeted to other than Earth, the default is to initiate the time-critical EDL sequence unless the s/c is in receipt of a ground-originated "no-go" command.

7.1.4 ***Deleted***

7.1.5 **Special Data Capture** - Sequences **shall** be designed to store on-board any special science and/or engineering data until confirmation of its safe receipt on the ground, in addition (for Type I) to transmitting the data in real time.

Rationale: The real time data link can be adversely affected by weather and/or loss of ground station, thus if data is special (e.g., unique), then it should be stored on-board.

Note: *The practice of calling the DSN to criticality A or B status, as an alternative to on-board data storage, is to be avoided.*

Note: *Mission-critical event flight data capture is addressed in Section 3.1.*

7.1.6 **Sequence Initial Conditions** - Sequence designs **shall** be based on an explicit understanding and/or establishment of the state of the spacecraft to assure proper sequence execution.

Rationale: It is important to establish the correct spacecraft configuration for proper sequence execution.

7.1.7 **Resource Margins for Stored Sequence Operations** - Operating margins **shall** be planned for system resources, including power, thermal, communications links, computer memory, timing, and throughput, and bus bandwidth, in all on-board stored sequence controlled activities.

Rationale: To maximize the prospects for safe, reliable operation.

7.2 Launch Scenario Design

7.2.1 **Sequence End State** - Completion of the launch sequence **shall** leave the spacecraft in a ground-commandable, safe state requiring no time-critical ground commanding to assure health and safety.

Note: *"Safe" connotes a positive power margin exists; the S/C thermal condition and inertial orientation are stable; viewing constraints, if any, are satisfied; S/C consumable resources (e.g., propellant, cryo supply) are preserved for the planned mission use; and the S/C is transmitting a downlink signal.*

Rationale: Defines the lowest risk approach by avoiding reliance on ground functions to achieve a sustainable condition.

Note: *The S/C should be safe without ground intervention for at least 10 days following S/C-L/V separation- to allow for ground equipment unavailability, e.g., due to failure, earthquake, etc.; plus ample time for the ground to diagnose and respond to unexpected S/C behavior and/or anomalous L/V performance, should such circumstances occur.*

7.3 Trajectory Correction Maneuver (TCM) Scenario Design

Note: *No design principles now exist for the subject scenario.*

7.4 Orbit Insertion Scenario Design

7.4.1 **Sequence End State** - Design and operations **shall** ensure that the spacecraft is left in a ground-commandable, safe state requiring no time-critical ground commanding to assure health and safety at the completion of the critical event (e.g., orbit insertion).

7.5 Entry, Descent & Landing (EDL) Scenario Design

Note: *No design principles now exist for the subject scenario.*

7.6 Aerobraking (A/B) Scenario Design

7.6.1 **Exit Conditions** - During the aerobraking phase of the mission, the spacecraft configuration(s) and operating mode(s), including all those possible from termination of the on-board activity, **shall** result in a safe condition for the aerobraking drag passes.

Rationale: Avoids reliance on timely ground intervention, which might not be possible.

7.6.2 **Aerobraking Aerostable Flight System Configuration** - The spacecraft configuration for aerobraking **shall**, without requiring active control, achieve and maintain a predictable and safe attitude, starting from any orientation and control mode, in the presence of drag forces.

7.6.3 **Aerobraking Thermal Margin** - The spacecraft design **shall** have positive margins to safe temperature limits in the presence of the peak expected heating rate, corresponding to 3-sigma atmospheric variability, over the duration of the drag pass.

Note: *Assumes worst-case orbital profile.*

7.6.4 **Aerobraking Required Operational Margins** - Aerobraking design and operations **shall** comply with the Table 7.6.4-1 margins at key milestones.

Per paragraph 6.3.1, Type 0 projects document alternative margins in the approved Project Plan.

Table 7.6.4-1 Aerobraking Operational Margins at Key Life Cycle Milestones

Parameter	MDR/PMSR	PDR	CDR	SIR	Launch
Peak Heating Rate Margin	125%	100%	75%	65%	50%

Note: *These margins apply to the peak expected heating rate during the drag pass given the worst-case orbital profile and 3-sigma atmospheric variability.*

Note: *Margin = 100%*{H/h - 1}*

where H = peak expected heating rate at which s/c temperature margin is zero, and

h = peak expected heating rate for the design point at the milestone.

Example: when h = 0.5 x H, 100% margin exists.

7.6.5 **Aerobraking Fault Protection Design** - No single failure during aerobraking **shall** (**not** required for Type II, *should* for Type 0) result in spacecraft temperatures exceeding maximum safe limits.

Note: *See 9.3.2*

8.0 Flight System Verification and Validation Design

8.1 General

8.1.1 Minimum Operating Times for Electronics Assemblies

8.1.1.1 Unit level prior to flight system integration

8.1.1.1.1 Each electronics assembly, including each side of a block redundant element, **shall** have 200 hours of operation prior to delivery flight system integration, excepting special cases per 8.1.1.1.2 and 8.1.1.1.3.

Rationale: The intent of this requirement is to screen workmanship defects prior to system-level testing and to confirm that the electronics assembly operates as designed and as expected.

Note: *The requirement also applies to electronics subassemblies, such as motor controllers and encoders.*

8.1.1.1.2 Science instruments **shall** have accumulated 300 hours of operation prior to delivery to flight system integration, unless it is planned that at least 300 hours of instrument operation will be accumulated in system-level testing, in which case science instruments **shall** have accumulated 200 hours of operation prior to delivery to flight system integration.

Rationale: Instruments are generally not operated in system-level testing as much as the engineering units are. The goal is to get 500 hours total operating time on instruments prior to launch, while recognizing that operating time in system testing will be limited.

8.1.1.1.3 Operating hours for wear life-limited items (such as moving mechanical assemblies with integrated electronics) may be tailored and **shall** be documented in the project's Mission Assurance Plan.

Rationale: Electronic components integrated in moving mechanical assemblies typically do not experience enough total operating hours to be compliant with the minimum 200- or 300-hour requirement. Embedded electronics that are not operated until integrated with wear life–limited mechanisms should be implemented with high-reliability electronics parts that are adequately screened (e.g., Class 2+ or better).

Note: *Operating hours are not accumulated merely by staying powered: The electronics must actively perform a function, such as testing that exercises the circuits, logic paths, intra-instrument interfaces, the interfaces between distributed instrument electronics and sensors, etc.*

8.1.1.2 **System level prior to launch** – System-level operating hours for all electronics assemblies are intended to exercise functions, modes, and interfaces.

8.1.1.2.1 Single-string electronic assemblies (except science instruments) **shall** have accumulated at the system level 1,000 hours of operation prior to launch.

8.1.1.2.2 Each side of a block redundant element **shall** have accumulated at the system level 500 hours of operation prior to launch, with a goal of 1,000 hours.

8.1.1.2.3 Science instruments **shall** have accumulated at the system level 200 hours of operation prior to launch.

8.1.1.2.4 System-level operating hours for wear life-limited items (such as moving mechanical assemblies with integrated

electronics) may be tailored and **shall** be documented in the project's Mission Assurance Plan.

Note: *The intent of this requirement is to adequately exercise the electronics in the system environment to identify and mitigate adverse system-wide interactions prior to launch. While the power-on operation at the system level acts to further burn-in piece parts, this is not the motivation for this requirement.*

8.1.2 **Handling and Test Constraints** - Flight system verification and validation **shall** be accomplished while adhering to the subsystem and assembly handling and test constraints provided via the hardware and software certification reviews held prior to delivery to ATLO.

Note: *Handling and test constraints include all cautions, warnings, and prohibitions together with any maintenance and servicing that may be necessary to ensure health, safety, and stress-free operation of the product in the system environment.*

Note: *Constraints are supplied to the ATLO organization prior to the product delivery to ensure that they can be met, or that the product can be designed consistent with achievable constraints.*

8.1.3 **Allocation and Tracking of Life Limited Items** - Flight system life limited items (e.g., reaction wheel revolutions, thermal cycles, valve actuations, etc.) **shall** be allocated and tracked during pre-launch testing to assure sufficient availability post-launch to meet mission objectives during flight operations.

Rationale: *Usage of life limited items needs to be tracked over their entire lifecycle (both pre-launch and post-launch). Margin must be included in the allocation because pre-launch testing may be more stressful than actual flight operations.*

Note: *Examples of life-limited items are reaction wheel revolutions, thermal cycles, valve actuations, battery charge/discharge cycles, etc.*

8.2 Pre-delivery Verification

8.2.1 **Subsystem and Assembly Level** - All flight hardware and software **shall** be functionally verified to conform to all allocated subsystem or assembly requirements (including EMC/EMI) prior to delivery to ATLO.

8.2.2 Early Interface Testing

a. Payload-to-spacecraft mechanical interfaces *should* be verified prior to the subsystem CDR, and early enough such that any incompatibility can be resolved without impacting the ATLO schedule.

Note: *For example, via early delivery of a mechanical mock-up or drill template*

b. Payload-to-spacecraft electrical interfaces, including protocol compatibility, *should* be verified prior to the subsystem CDR, and early enough such that any incompatibility can be resolved without impacting the ATLO schedule.

Note: *For example, via early use of electrical interface simulators with breadboards*

8.2.3 **System Level** - Unique operations and procedures to be used at the launch site, or during environmental testing **shall** be dry run sufficiently in advance of the actual operation to permit corrective action be taken to the results obtained and re-verification prior to the planned use with the flight article in order that there be no impact to the ATLO schedule.

8.2.3.1 **Launch site long umbilical lines** - Prior to shipment to the launch site, proper operation of the spacecraft with the long umbilical lines to be used at the launch site **shall** be demonstrated.

8.2.3.2 **Launch site support equipment** - Prior to shipment to the launch site, proper operation of the GSE to be used at the launch site with the spacecraft **shall** be demonstrated.

8.3 System Assembly, Integration and Test

8.3.1 System Assembly

8.3.1.1 **Two-person rule** - System assembly and test of flight hardware **shall** adhere to the “two person rule.” Each operation or observation/measurement performed on flight hardware **shall** be verified by a second set of eyes.

Rationale: The physical presence of two persons for “hands on” operations (e.g., torquing of fasteners or mating of electrical connectors) is required for the safety of personnel and flight hardware.

8.3.2 System Integration

8.3.2.1 **Safe-to-mate verification** - A “safe-to-mate” verification **shall** be performed after assembly of hardware into the flight system and before electrical connections are made and the hardware powered.

Rationale: The safe-to-mate verification ensures that flight hardware being integrated is not subjected to out of specification conditions.

8.3.2.2 **Software regression testing** - New versions of flight software delivered to ATLO **shall** undergo regression testing on the flight vehicle prior to use in system level verification.

Note: *Regression testing demonstrates that there are no obvious, unintended changes to the software, and verifies the functionality of capabilities new in this delivery.*

Note: *The regression test is not a substitute for thorough pre-delivery verification of the flight software on testbeds.*

Rationale: If the flight software used in system level verification of a flight system is later found to be defective, it may invalidate the completed testing.

8.3.3 System Functional Verification

System functional verification refers to the highest level of assembly. However, Engineering Delivery Tasks (EDTs) limit the scope of work to partial systems and do not include authority over higher level system decisions. Therefore, this design control only applies to the extent possible within the scope of work context.

8.3.3.1 **“Plugs out” test** - system level electrical “plugs-out” testing using the minimum number of test equipment connections **shall** be performed.

Note: *Support equipment connections should be limited to those that are unavoidable. Deviations from the flight conditions are documented, and a risk assessment included in the Test-As-You-Fly Exceptions.*

Rationale: The "plugs out" test confirms that the system operates properly without support equipment or umbilical connections. Plugs out testing also confirms that the system operates in the various spacecraft configurations encountered during the mission, e.g., those resulting from

in-flight events such as launch vehicle separation, Entry, Descent, and Landing (EDL), probe separation, etc.

8.3.3.2 **Deployments and articulations** - Verification of all deployable or movable appendages and mechanisms **shall** include full-range articulation, unless such testing presents a significant risk to flight hardware, e.g., due to gravity, in which case first motion testing **shall** be performed in the fully integrated system configuration with full range articulation done prior to delivery using MGSE to offset gravity effects.

Rationale: Demonstrates freedom from mechanical interferences after environmental exposure and in the final flight configuration.

Note: *To the extent possible, deployments and articulations are to be performed in a flight-like manner.*

8.3.3.3 **Mechanical clearances** - Verification by visual inspection of mechanical clearances and margins (e.g., potential reduced clearances after blanket expansion in vacuum) **shall** be performed on the final as-built hardware.

Rationale: To verify the adequacy of thermal blanket clearances, etc. before and after environmental test, handling, etc.

8.3.3.4 **Long duration test of flight system** - Verification of the flight system **shall** include an uninterrupted long duration test of at least one week performed at the system level during which the design is demonstrated to be free of defects that could be masked in routinely restarting the system, as is typical in a test program.

Note: *The system is expected to be operated through all mission phases and transitions.*

8.3.3.5 **Phasing test** - Phasing tests **shall** be performed in the final flight configuration to verify proper operation of polarity-sensitive functions, including software (both flight and ground) and command and control functions.

Note: *Participation by the GN&C analyst is essential for ensuring a complete and accurate understanding of the proper phasing.*

8.3.3.6 **System alignments** - System alignment verifications **shall** be performed before and after exposure to system environmental testing.

Rationale: Confirms that there were no shifts in alignments as a result of environments and that the post-environmental alignments are acceptable for flight.

8.3.3.7 ***Deleted***

8.3.3.8 **Long duration test for instrument projects** - Verification of instruments **shall** include an uninterrupted, long duration test at the instrument level, demonstrating flight-like operations over at least 1x the longest planned, continuous, in-flight instrument operating scenario duration for instruments that are operated intermittently, or a minimum of 72 hours for instruments that are operating continuously over the mission duration.

Note: *The longest planned, continuous, in-flight operating scenario is taken here to mean the longest operating scenario in which there is no planned opportunity for ground intervention (e.g., to reset the instrument and transition back to its operating mode) within the planned mission ops concept.*

Note: *This design rule is applicable to JPL instrument projects where the instrument is delivered to another JPL project, another NASA Center, or another agency (see FPP 5.1.2). A related design rule, 8.3.3.4, is applicable at the flight-system level for projects in which JPL has the responsibility for flight system integration and test.*

Note: *This instrument-level test is not intended to meet electrical part level burn-in or infant mortality screening, which should generally be performed as early as possible in the development cycle and at the lowest practical level of assembly.*

Rationale: The long duration test is responsive to test-as-you-fly principles and is intended to demonstrate that the design is free of anomalies that could be masked in routinely restarting the system, as may occur in routine ground testing (e.g., counter roll-over issues, sequence crashes, ring buffer recycle problems, memory leaks, file management system issues, etc.). A minimum 72-hour duration for continuously operated instruments is established to ensure that the test is sufficiently long compared to typical ground tests to provide a reasonable likelihood of detection of such anomalies.

8.3.4 Flight Sequence Verification

8.3.4.1 **Sequence integrity** - Flight system verification and validation **shall** include use of MOS-generated sequences as identical to flight sequences as possible.

Rationale: Verifies the sequence generation processes end to end through execution on the spacecraft.

Note: *Deviations from flight sequences are documented, and a risk assessment included in the Test-As-You-Fly Exceptions.*

8.3.4.2 **Verification on a testbed** - All flight sequences that will be run on the flight vehicle in ATLO **shall** first be run on a system testbed.

Rationale: Ensures safety of the flight vehicle, and eliminates potential impacts to system testing schedule that could occur with untested products.

8.3.5 System Fault Protection Verification

8.3.5.1 **Effectiveness of system redundancy management** - When redundancy has been used in the flight system design to provide fault tolerance, system fault protection testing **shall** verify that the redundancy management actions result in timely preservation/restoration of required system functionality. As a minimum, testing of redundancy management **shall** be performed while executing critical mission scenarios.

8.3.6 System Stress Testing

8.3.6.1 **General** - Stress testing **shall** be used to demonstrate the robustness of the flight system design. Stress testing **shall** address testing, as a minimum, single faults that cause multiple-fault symptoms, and occurrences of subsequent faults in an already faulted state.

Rationale: Demonstrates the capability of the system to maintain functionality in the presence of arbitrary initial conditions such as when the system has already experienced faults or other off-nominal conditions.

8.3.7 System Environmental Verification

8.3.7.1 **Environmental exposure fault isolation** - Sufficient flight system functional testing **shall** be performed integral to environmental testing

to know with certainty the pass/fail result of exposure to each of the environments.

8.3.7.2 **Temperature-dependent calibrations** - Thermostatic control settings and temperature telemetry calibrations **shall** be verified during thermal testing.

8.3.8 Inter-System Verification

8.3.8.1 **Mechanical fit check** - Early verification of the mechanical interface between flight system and launch vehicle **shall** be performed using a high fidelity mechanical mock-up or the flight interface hardware prior to shipment to the launch site, sufficiently in advance to permit recovery from an unexpected incompatibility.

8.3.8.2 **Electrical interface check**- Early verification of the electrical interfaces between the flight system and launch vehicle **shall** be performed prior to S/C-L/V Interface Control Document (ICD) sign-off, and sufficiently in advance of integrated operations to be able to recover from any unexpected incompatibility.

Rationale: An electrical interface check is performed early since an incompatibility might necessitate change(s) to s/c electronics, and if discovered later could result in adversely impacting the ATLO schedule.

8.4 Launch Operations

8.4.1 Pre-mate Verification

8.4.1.1 **Post-ship functional test** - The flight system **shall** be functionally tested after delivery to the launch site and prior to mating with the launch vehicle.

Rationale: Confirms that no functional failures occurred during shipment and/or reassembly.

8.4.2 Post-mate Verification

8.4.2.1 **Red tag items** - An inventory of 'remove before flight' and 'install before flight' items **shall** be developed and tracked during launch processing. Red tag items (also known as “remove before flight” items) **shall** be photographed after removal, and the photographs retained as part of the ATLO records. In-process close-out photographs of the spacecraft in the final configuration that clearly

indicate the status of 'remove before flight' and 'install before flight' items **shall** be taken and retained as a part of the ATLO records.

Note: *This provides proof that these critical steps in preparation for launch were in fact completed.*

8.4.3 **Launch-critical Support Equipment**

8.4.3.1 **Availability** - No single failure in support equipment required to condition the s/c for launch **shall** cause a launch delay greater than 48 hours.

Rationale: Concerns are for erosion of a limited launch period, and the potential for needing to off-load launch vehicle propellants should rapid repair not be possible.

Note: *Limiting the s/c conditioning late in the countdown minimizes the dependency on support equipment functionality, and thus the need for tested spare units.*

8.4.3.2 **Fault propagation** - No single failure in support equipment used with the spacecraft at the launch pad **shall**:

a. place the spacecraft in a condition inconsistent with the launch sequence (e.g., by resetting to the “safe” condition or releasing safety inhibits for launch), and/or
b. simulate conditions (e.g., lift-off, S/C-L/V separation) that result in the spacecraft initiating the launch sequence.

9.0 Flight System Flight Operations Design

It is important that after launch projects operate the flight system in a manner that is consistent with the principles that guided its design and testing pre-launch. This section contains the principles projects ***should*** follow to ensure that operation. Project operations personnel ***should*** periodically review these principles to ensure consistent operations, but especially when approaching mission critical events and mission extensions.

9.1 General

9.1.1 **Communication during mission-critical events** - (Ref. Design Principle (DP) 3.1.2)

Note: *Mission-critical events are those that if not executed properly and in a timely manner could result in failure to achieve mission success, e.g., orbit insertion; entry, descent, and landing. A Trajectory Correction Maneuver*

(TCM) is not mission-critical unless it must execute properly in the time scheduled for it, i.e., cannot be delayed.

9.1.1.1 **Downlink during critical events (Ref. DP 3.1.2.1)** - Post-launch operations **shall** (*should* for Type II and Type 0) provide a real-time downlink during mission-critical events.

Note: *Communications during other special mission events is addressed in 9.1.3.*

9.1.1.2 **Redundant ground system data paths (Ref. DP 3.1.2.2)** - Post-launch operations **shall** (*should* for Type II and Type 0) ensure that no single ground system failure results in loss of flight data from mission-critical events.

Note: *Scheduling of mission critical events to occur during the overlap of 2 tracking complexes is one way to satisfy this requirement. A direct-to-earth link to one tracking complex, plus a UHF link to an orbiting asset that relays the data to another tracking complex is another way to satisfy this requirement.*

Note: *Implementation of this principle may not be practical or possible for Earth orbiting missions.*

9.1.1.3 **Redundant ground to spacecraft data paths** - Post-launch operations *should* ensure that no single ground system failure results in loss of capability to uplink commands to the flight system during mission critical events.

Note: *Scheduling of mission critical events to occur during the overlap of 2 tracking complexes is one way to satisfy this requirement.*

9.1.2 **Protection of critical data (Ref. DP 3.1.3)** - Post-launch operations **shall** (*should* for Type II and Type 0) ensure that recovery of science and/or engineering data deemed critical to mission success not be dependent upon the availability of a single tracking complex.

Note: *On-board storage for later (re)transmission to Earth provides protection against loss of the real time link.*

9.1.3 **Telecommunications availability for mission - defined special activities (Ref. DP 4.5.1.4)** - Post-launch operations **shall** (*should* for Type II and Type 0) provide telemetry, command, and radiometric data capability during mission-defined special activities, such as all first uses of flight system functionality and all irreversible events.

Rationale: Provides real-time monitoring during mission-defined special activities, and timely contingency commanding in the event that unexpected behavior is observed.

Note: *Irreversible events are defined as those that change the flight system configuration in a way that cannot be undone (e.g., pyro firings, one-time deployments, like solar arrays or instrument covers, etc.).*

Note: *When switching of spacecraft components is required to provide the telecommunications capability for the mission-defined special activity, there is a risk trade between the benefit of having the visibility and the risks associated with the switching.*

9.1.4 **Telemetry visibility of spacecraft state (Ref. DP 4.4.6.4)** - Post-launch operations **shall** be able to determine rapidly and unambiguously the state of the flight system, particularly to determine if the spacecraft executed a fault protection response.

Note: *This enables ground operators to respond in a timely fashion to unexpected flight system states.*

9.1.5 ***Deleted***

9.1.6 **In-flight characterization (Ref. DP 4.1.7.2)** - Post-launch operations *should* perform in-flight demonstration of flight system functional capability prior to the actual mission need in order to characterize and evaluate the flight system and ground system end-to-end operation.

Note: *Early characterization/evaluation enables the project to identify flight/ground system shortfalls, and make changes safely and reliably with minimal threat to the mission.*

9.1.7 ***Deleted***

9.1.8 **Protection against errors (Ref. DP 4.1.3.2)** - Post-launch operations **shall** protect against errors that could result in loss of mission or significant impact to mission success by:

- following established procedures,
- only using validated and configuration controlled ground hardware and software,
- maintaining proficiency of current personnel and training new personnel, and
- validating and updating flight system models.

Note: *Flight system models should include instrument models that provide insight into instrument commands and consumables usage.*

9.1.9 **Stressing ground operations capability demonstration** - Post-launch operations *should* perform demonstration of ground system stressing operations cases prior to the actual mission need for those operations.

Note: *Early demonstration of ground system stressing operations cases enables the project to identify shortfalls and make changes with minimal threat to the mission.*

9.2 Flight Software Operation

9.2.1 ***Deleted***

9.2.2 **Post-launch flight software update rigor and process** - The post-launch operations design and implementation process **shall** ensure that the update of flight software is performed with the same rigor (review, testing, safeguards, operations procedures, etc.) as is applied during pre-launch flight software development, including functional testing of updated code on a testbed.

9.2.3 **In-flight on-board flight parameter update** - The post-launch operations design and implementation process **shall** ensure that the update of critical on-board parameters is performed with the same rigor (review, testing, safeguards, operations procedures, etc.) as is applied to pre-launch parameter selection, including functional testing on a testbed prior to uplink.

Note: *Critical on-board parameters in this context means those that have a fundamental effect on nominal or fault protection performance of the spacecraft. Specifically not included are updates to parameters that are made as part of the normal sequence development process.*

9.3 Flight Hardware Operation

9.3.1 **Powering off the RF Downlink** - During nominal flight operations, the spacecraft downlink RF transmitter hardware (e.g., exciters, power amp) **shall** remain “on” during nominal flight operations (not required for Type II, *should* for Type 0) and have a downlink signal transmitted continuously during the entire mission. Exceptions are (a) the momentary cycling of power to the transmitter chain hardware that may result via system autonomous fault protection responses, and (b) when cycling is essential to mission viability and the risk is demonstrated to be acceptable.

Rationale: *It is desirable to always have a downlink signal to verify nominal events and to facilitate anomaly analysis and resolution.*

Note: *Earth orbiting and surface missions on other solar system bodies are cases where exception (b) above is likely to apply.*

9.3.2 **Powering off the RF Receiver** - During nominal flight operations, the spacecraft RF receiver hardware **shall** remain "on" unless cycling is essential to mission viability and the risk is demonstrated to be acceptable.

Rationale: It is desirable to always have a spacecraft capability for command receipt in the event ground intervention is required.

9.3.3 ***Deleted***

9.3.4 ***Deleted***

9.3.5 ***Deleted***

9.3.6 **Simultaneous use of Prime and Redundant Hardware** - Simultaneous use of selected prime and redundant hardware to enhance reliability/performance for accomplishing mission critical activities **shall** be considered only after the operation has been verified and validated, and **shall** be approved at the Critical Events Readiness Review (or alternate appropriate review for Type 0).

Note: *Part of this decision needs to be a value vs. risk trade, including verifying by test that the configuration using both prime and redundant units does no harm to the nominal spacecraft operations.*

9.3.7 ***Deleted***

9.3.8 ***Deleted***

9.4 Flight Scenario/Sequence Design

9.4.1 ***Deleted***

9.4.2 **Critical Event Telemetry Monitoring (Operations) (Ref. DP 7.1.2)** - Post-launch operations **shall** (*should* for Type II and Type 0) design scenarios/sequences such that mission-critical event data and mission-critical deployments are monitored via real-time telemetry.

Rationale: Real time critical event telemetry is needed to monitor that the event occurs as planned, or if not, to determine why not.

9.4.3 ***Deleted***

9.4.4 ***Deleted***

9.4.5 **Special Data Capture (Operations) (Ref. DP 7.1.5)** - Post-launch operations **shall** design sequences to store on-board any special (e.g., unique, single acquisition opportunity) science and/or engineering data until confirmation of its safe receipt on the ground, in addition to transmitting the data in real time.

Rationale: The real time data link can be adversely affected by weather and/or loss of ground station, thus if data is special (e.g., unique), then it should be stored on-board.

Note: *The practice of calling the DSN/NEN to criticality A or B status, as an alternative to on-board data storage, is to be avoided.*

Note: *Mission-critical event flight data capture is addressed in Section 9.1.*

9.4.6 **Sequence Initial Conditions (Operations) (Ref. DP 7.1.6)** - Post-launch operations and sequence design **shall** understand and/or establish an explicit state of the flight system to assure proper sequence execution.

Rationale: It is important to establish the correct spacecraft configuration for proper sequence execution.

9.4.7 ***Deleted***

9.4.8 ***Deleted***

9.4.9 ***Deleted***

9.4.10 ***Deleted***

9.5 Operating Margins

9.5.1 **Operating Margins for Real Time Operations** - Post-launch operations **shall** plan, maintain, and monitor operating margins for system resources, (e.g., power; thermal; communications links; computer memory, timing, and throughput; bus bandwidth; and fault protection thresholds and persistences) in all flight system activities.

Rationale: To maximize the prospects for safe, reliable operation.

Note: *Margins help solve problems and mitigate risk.*