LPR 7123.1

Effective Date: July 20, 2010

Revised: July 9, 2012

Expiration Date: January 31, 2015

Langley Research Center

LaRC Systems Engineering Processes and Requirements

National Aeronautics and Space Administration

DOCUMENT HISTORY LOG

Document Revision	Effective Date	Description
A	July 20, 2010	Baseline
A-2	June 12, 2012	Added Appendix G

Contents

P.1 PURPOSE 4
P.2 APPLICABILITY 4
P.3 AUTHORITY 4
P.4 APPLICABLE DOCUMENTS AND FORMS 4
P.5 MEASUREMENT/VERIFICATION 5
P.6 CANCELLATION 5
1. RESPONSIBILITIES 6
2. PROCEDURE 8
2.1 Program/Project/Task Systems Engineering 8
2.2 The Systems Engineering Management Plan (SEMP) 8
2.3 Systems Engineering Common Technical Processes 10
3. RECORDS 11
4. TAILORING AND WAIVERS 11
APPENDIX A. DEFINITIONS 13
APPENDIX B. ACRONYMS 14
APPENDIX C. REQUIREMENTS LIST FOR THIS LPR 15
APPENDIX D. CLASS OF PROGRAM/PROJECT/TASK 16
APPENDIX E. COMMON TECHNICAL PROCESSES BEST PRACTICES 18
E.1 Overview 18
E.2 Systems Engineering Common Technical Processes 19
APPENDIX F. REFERENCES 36
APPENDIX G. LaRC SPECIFIC ENGINEERING BEST PRACTICES 37

PREFACE

P.1 PURPOSE

P.1.1 This Langley Procedural Requirements (LPR) document implements the Agency Systems Engineering Management requirements documented in NASA Procedural Requirements (NPR) 7123.1A Appendix C. These processes focus on defining stakeholder expectations and implementing a systematic approach for satisfying those expectations. The processes are extracted from industry, national, international, and Agency standards. These processes provide the best typical practices currently available.

P.2 APPLICABILITY

P.2.1 This LPR applies to the personnel, programs, projects, and tasks at LaRC, including contractors to the extent specified in their respective contracts or agreements. ("Contractors," for purposes of this paragraph, include contractors, grantees, Cooperative Agreement recipients, Space Act Agreement partners, or other agreement parties.)

P.2.2 This LPR applies to all Programs, Projects and Tasks conducted by LaRC that are governed by NPR 7120.5, *NASA Spaceflight Program and Project Management Requirements*. This LPR also applies to all Institutional Infrastructure Programs, Projects, and Tasks conducted by LaRC (with the exception of environmental compliance and restoration activities), that are governed by NPR 7120.7, *NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements*. In addition, this LPR applies to Technology Development Programs, Projects, and Tasks conducted by LaRC that are governed by NPR 7120.8, *NASA Research and Technology Program and Project Management Requirements*.

P.3 AUTHORITY

42 U.S.C. 2473(c) (1), Section 203(c) (1) of the National Aeronautics and Space Act of 1958, as amended.

P.4 APPLICABLE DOCUMENTS AND FORMS

a. NPR 7120.5, NASA Space Flight Program and Projects Management Requirements

b. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements

c. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements

d. NPR 7123.1, NASA Systems Engineering Processes and Requirements

e. NPR 7150.2, NASA Software Engineering Requirements

f. LAPD 7000.2, Review Program for Langley Research Center (LaRC) Facility Projects

g. LPR 1440.7, LaRC Records Management Procedural Requirements

h. LPR 5000.2, Procurement Initiator's Guide

i. LPR 5300.1, Product Assurance Plan

j. LPR 7120.5, Space Flight Project Practices Handbook

k. LPR 7130, Project and Task Review Procedural Requirements

l. LPR 7120.7, Space Flight Independent Life Cycle Review Procedural Requirements

m. LPR 8040.1, Flight Projects Directorate Space Flight Configuration Management Requirements

n. LMS-CP-1725, Export Control

o. LMS-CP-2310, Electronic Storage and Archival Systems (Document and Data Management)

p. LMS-CP-4756, Handling, Preservation, Storage, and Shipping of Space Flight Hardware

q. LMS-CP-5526, Product Requirements Development and Management Procedures

P.5 MEASUREMENT/VERIFICATION

Verification will be accomplished by inspection as part of the LaRC Internal Audit process.

P.6 CANCELLATION

None

Original signed on file
Cynthia C. Lee
Associate Director

Approved for public release via the Langley Management System. Distribution is unlimited.

1. RESPONSIBILITIES

1.1 The LaRC Center Director, or designee, is responsible for the implementation of the SE policies, processes, and procedures at LaRC.

1.2 The Chair of the LaRC Center Management Council (CMC), or designee, serves as the LaRC Designated Governing Authority (DGA) to approve systems engineering implementation for LaRC Class 1 Programs/Projects/Tasks (see Appendix D for Program/Project/Task Class descriptions).

1.3 The LaRC Chief Engineer, or designee:

1.3.1 Serves as the LaRC DGA to approve systems engineering implementation of LaRC Class 2 and 3 Programs/Projects/Tasks;

1.3.2 Reviews Class 1 Programs/Projects/Tasks systems engineering implementation prior to DGA review/approval; and

1.3.3 Ensures the appropriate Engineering Directorates review the Systems Engineering Management Plan (SEMP) (for a Class 1 or Class 2 Program/Project/Task) or other appropriate documentation of systems engineering implementation plans (for a Class 3 Program/Project/Task).

1.4 The Program/Project/Task Manager (PM), or designee:

1.4.1 Ensures a SEMP (for a Class 1 or Class 2 Program/Project/Task) or other appropriate documentation (for a Class 3 or Class 4 Program/Project/Task) is written to define Program/Project/Task implementation of SE requirements and processes;

1.4.2 Ensures review and approval of the SEMP or other appropriate documentation by the appropriate SE DGA;

1.4.3 Controls the SEMP or other appropriate documentation under Program/Project/Task control processes;

1.4.4 Provides the design team with statutory, regulatory, and Agency mandatory requirements, relevant information from previous similar designs, and any other requirements for product design and development.

1.4.5 Ensures that software developed within NASA or acquired complies with NPR 7150.2, for systems that contain software (see NPR 7123.1, Section 6.2.6).

1.5 The Program/Project/Task Systems Engineering Team (SET):

1.5.1 Prepares the SEMP;

1.5.2 Executes or oversees the execution of the Program/Project/Task systems engineering tasks.

1.6 The Director of the engineering organization providing the Program/Project/Task Chief Engineer (or Lead Systems Engineer if no Chief Engineer), or designee:

1.6.1 Ensures the Chief Engineer (or Lead Systems Engineer or other appropriate person) for the Program/Project/Task prepares the SEMP (for a Class 1 or Class 2 Program/Project/Task) or other appropriate documentation (for a Class 3 or Class 4 Program/Project/Task) in accordance with this LPR.

1.6.2 Ensures all engineering directorates involved in the engineering work of the Program/Project/Task concur on the SEMP or other appropriate documentation.

1.6.3 Ensures compliance with the approved SEMP or other appropriate documentation.

1.6.4 Approves the plans for systems engineering implementation for Class 4 Programs/Projects/Tasks.

1.7 For Programs/Projects/Tasks involving more than one Center, the lead organization develops documentation to describe the hierarchy and reconciliation of plans for implementing system engineering processes and requirements that are applicable to all Centers involved. However, the LaRC Center Director, Engineering Director and Chief Engineer are responsible to ensure all LaRC work in support of these efforts is in compliance with this LPR and NPR 7123.1.

1.8 Responsibilities for various activities associated with the SEMP or other appropriate documentation of the systems engineering implementation are summarized in Table 1-1.

	Class 1	**Class 2**	**Class 3**	**Class 4**
CMC Chair	Approves			
Chief Engineer	Reviews	Approves	Approves	
Program/Project/Task Manager	Concurs	Concurs	Concurs	Concurs
Engineering Director	Reviews	Reviews	Reviews	Approves
Systems Engineering Team	Prepares	Prepares	Prepares	Prepares

Table 1-1 Responsibilities for the SEMP or alternative documentation of systems engineering implementation

2. PROCEDURE

2.1 Program/Project/Task Systems Engineering

2.1.1 The Program/Project/Task Systems Engineering Life-cycle is defined as a set of activities, processes and reviews that enables the smooth, incremental development of products essential to successfully achieving the Program/Project/Task goals.

2.2 The Systems Engineering Management Plan (SEMP)

2.2.1 The purpose of a SEMP is to provide a single, integrated technical planning document which addresses the systems engineering management and implementation for systems and subsystems for in-house and contracted Programs/Projects/Tasks.

Req. 001: Each Class 1, and 2 Program/Project/Task (refer to Appendix D) SET shall provide to the DGA a SEMP as described in Appendix D.4 “SEMP Annotated Outline” of NPR 7123.1, NASA Systems Engineering Processes and Requirements.”

Rationale: [The SEMP is required by NPR 7123.1. The SEMP provides the specifics of the technical effort and describes what technical processes will be used, how the processes will be applied, how the project will be organized to accomplish its activities, and the cost and schedule associated with accomplishing the activities. At LaRC, a stand-alone SEMP is required for any Class 1 and 2 Program/Project/Task because of their size and/or visibility.]

Trace: [NPR 7123.1 Sections 3.13, 6.2.1, 6.2.2]

Allocation: [LPR 7120.5, LPR 7120.7]

Verification Method: [Inspection]

Req. 002: Each Class 3 and Class 4 Program/Project/Task SET shall provide to the DGA the documentation of the material typically found in a SEMP (see Appendix D.4 “SEMP Annotated Outline” of NPR 7123.1) in the manner and form agreed to with the DGA.

Rationale: [Smaller projects do not have the resources to develop a full SEMP, so the DGA decides what needs to be documented and the form that documentation will take. For example, the material may be documented in the project plan, as an appendix to the project plan, or in some other appropriate form as determined by the DGA.]

Trace: [NPR 7123.1 Sections 3.1.3, 6.2.1, 6.2.2]

Allocation: [LPR 7120.5, LPR 7120.7]

Verification Method: [Inspection]

2.2.2 The SEMP and the project plan are coordinated to ensure compatibility with the allocated resources/enabling products (cost, schedule, personnel, and facilities), milestones and deliverables. The SEMP is used to identify and evaluate the required technical teams' performances. The SEMP is also used in the technical risk assessment and deriving the progress measurement criteria.

2.2.3 For projects with significant portions of the engineering work contracted out, the LaRC SEMP scopes and plans the NASA portion of the project implementation of the systems engineering common technical processes before, during and at the completion of the contracted effort. This includes planning the technical team's involvement in the Request for Proposal (RFP) preparation, in source selection activities, acceptance of deliverables, and storage and disposal of residual hardware.

2.2.3.1 Depending upon the scope and content of the contracted effort, a contractor may be required to develop and maintain a SEMP or other appropriate documentation for their contracted effort.

2.2.4 SEMP Maintenance

Req. 003: Each Program/Project/Task SET shall update the SEMP (or alternate documentation as required in Req. 002), prior to each Program/Project/Task lifecycle review.

Rationale: [The SEMP (or alternate documentation) is not as useful if it is outdated. The update is necessary for DGA approval at the review (see Req. 004).]

Trace: [NPR 7123.1 section 6.2.4]

Allocation: []

Verification Method: [Inspection]

Req. 004: The DGA shall review and approve or disapprove the SEMP (or alternate documentation as required in Req. 002) at each Program/Project/Task lifecycle review.

Rationale: [The SEMP (or alternate documentation) is not as useful if it is outdated. Approval at this frequency is required by NPR 7123.1.]

Trace: [NPR 7123.1 section 6.2.3]

Allocation: []

Verification Method: [Inspection]

2.3 Systems Engineering Common Technical Processes

2.3.1 The implementation of the 17 Common Technical Processes are described in the SEMP (or alternate documentation) as discussed in NPR 7123.1, Appendix D.4.6. The LaRC tailoring of the best practices described in NPR 7123.1, Appendix C, are enumerated in Appendix E of this LPR. Additional information about these 17 processes is provided in NASA/SP-2007-6105 (which can be found on the NASA Technical Reports Server at: http://ntrs.nasa.gov/search.jsp?R=140111&id=5&as=false&or=false&qs=Ntt%3DSystems%2BEngineering%2BHandbook%26Ntk%3DTitle%26Ntx%3Dmode%2Bmatchall%26Ns%3DHarvestDate%257c1%26N%3D0).

Req. 005: Each Class 1, and 2 Program/Project/Task SET shall follow the best practices enumerated in Appendix E.2 of this document for each of the 17 Common Technical Processes unless the SEMP documents reason(s) for not following particular practice(s).

Rationale: [These best practices are extracted from industry, national, international, and agency standards. In general, they should be used on Class 1 and 2 Programs/Projects/Tasks. However, the individuality of each Program/Project/Task is appreciated and some practices that work for some Programs/Projects/Tasks do not work well for others, hence the intent of this requirement to give the Program/Project/Task sufficient flexibility to define the practices that they will follow subject to documenting reasons why any of the practices in Appendix E.2 will not be followed. For instance, the SET may conclude that the overhead associated with particular practices, or perhaps even entire processes exceed the benefit derived from particular practices, or they may conclude that alternative practices are better suited to the Program/Project/Task.]

Trace: [NPR 7123.1 Sections 3.1.3, 3.2.1.1, 3.2.2.1, 3.2.3.1, 3.2.4.1, 3.2.5.1, 3.2.6.1, 3.2.7.1, 3.2.8.1, 3.2.9.1, 3.2.10.1, 3.2.11.1, 3.2.12.1, 3.2.13.1, 3.2.14.1, 3.2.15.1, 3.2.16.1, 3.2.17.1]

Allocation: [LPR 7120.5, CP-5526, LPR 5000.2, LPR 5300.1, CP-4756, LPR 1440.7, LPR 8040.1, CP-1725, CP-2310, LPR 7120.7, LPR 7130, LAPD 7000.2, CP-5621]

Verification Method: [Inspection]

2.3.2 Because Class 3 and 4 Programs/Projects/Tasks are typically more resource-constrained then Class 1 and 2 Programs/Projects/Tasks, their SETs are not

required to document reasons for departing from the practices of Appendix E.2. However, Req. 002 still requires that they document the practices they will follow for the 17 Common Technical Processes.

2.3.3 Approval of the SEMP by the DGA constitutes approval of the systems engineering technical processes described in the SEMP. However, the SEMP cannot be used to grant relief from requirements outside of this LPR. Waivers and/or tailoring of requirements specified in other documents are required to follow the waiver and/or tailoring requirements of those other documents.

3. RECORDS

The following records are required by this LPR:

Record	Custodian
SEMP or other equivalent documentation	PM or designee

Additional records may be required, depending upon the detailed contents of the SEMP (or equivalent documentation).

4. TAILORING AND WAIVERS

4.1 Waivers to requirements specific to this LPR can be granted by the LaRC Center Director or his/her designee.

Req. 006: The PM of the Program/Project/Task shall provide any waiver requests to the LaRC Center Director (or designee) in writing, signed by the PM, and accompanied by evidence of concurrence by the relevant Project Chief Engineer or the Project Lead Systems Engineer and the Program/Project/Task sponsor (the Principal Investigator or other appropriate person).

Rationale: [The request is in writing to ensure a document trail. The signature of the PM ensures his/her awareness and support of the waiver request. The concurrence of the Project Chief Engineer or the Project Lead Systems Engineer ensures that the engineering aspects have been reviewed. The concurrence of the sponsor ensures that the sponsor is aware of the request – i.e., there is an informed customer.]

Trace: []

Allocation: []

Verification Method: [Inspection]

4.2 In cases where the identity of the Project Chief Engineer or Project Lead Systems Engineer and/or the Project sponsor are unclear, the LaRC Chief Engineer or his/her designee may assign individuals to act in those roles or may waive the requirement for concurrence.

Req. 007: The PM of the Program/Project/Task shall maintain all waiver documentation.

Rationale: [The Program/Project/Task is the responsible party for maintaining project documentation.]

Trace: []

Allocation: []

Verification Method: [Inspection]

4.3 Any tailoring or waivers to requirements of this LPR involving other LMS documents will be approved in accordance with the tailoring or waiver processes applicable to those LMS documents.

APPENDIX A. DEFINITIONS

A.1 Customer – The organization or individual that has requested a product and will receive the product to be delivered. The customer may be an end user of the product, the acquiring agent for the end user, or the requestor of the work products from a technical effort. Each product within the system hierarchy has a customer.

A.2 Designated Governing Authority – The management entity above the program, project, or task level with technical oversight responsibility.

A.3 Measure of Effectiveness (MOE) – A measure by which a stakeholder's expectations are judged in assessing satisfaction with products and systems produced and delivered in accordance with the associated technical effort. The MOE is deemed to be critical to not only the acceptability of the product by the stakeholder, but also critical to the operational / mission usage. An MOE is typically qualitative in nature or not able to be used directly as a "design-to" requirement.

A.4 Measure of Performance (MOP) – A quantitative measure that, when met by the design solution, will help ensure that an MOE for a product or system will be satisfied. These MOPs are given special attention during design to ensure that the MOEs to which they are associated are met. There are generally two or more measures of performance for each MOE.

A.5 Stakeholder – A group or individual who is affected by or in some way accountable for the outcome of an undertaking. Stakeholders include all who are involved in the Program/Project/Task – end-users, designers, manufacturing, test, and quality personnel, including those who may not be directly involved with doing the processing work.

A.6 Technical Requirements – Statements defining necessary performance characteristics of a product. Technical requirements are stated in a verifiable manner such that pass/fail or quantitative assessment criteria are specified.

A.7 Validation – Testing, possibly under simulated conditions, to ensure that a finished product works as required.

A.8 Validation (of a product) – Proof that the product accomplishes the intended purpose. Validation may be determined by a combination of test, analysis, and demonstration.

A.9 Verification – The process of proving or demonstrating that a finished product meets design specifications and requirements.

A.10 Verification (of a product) – Proof of compliance with specifications. Verification may be determined by test, analysis, demonstration, and inspection.

APPENDIX B. ACRONYMS

CMC	Center Management Council
CP	Center Procedure
DGA	Designated Governing Authority
LAPD	Langley Policy Directive
LaRC	Langley Research Center
LCC	Life-Cycle Cost
LMS	Langley Management System
LPR	Langley Procedural Requirements
MOE	Measure of Effectiveness
MOP	Measure of Performance
NASA	National Aeronautics and Space Administration
NPR	NASA Procedural Requirements
PM	Program, Project or Task Manager
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SET	Systems Engineering Team
WBS	Work Breakdown Structure

APPENDIX C. REQUIREMENTS LIST FOR THIS LPR

Requirement Number	Prior Paragraph Number	Description (these are abbreviated, the full text of the LPR paragraph apply)
001	2.2.1	Each Class 1, and 2 Program/Project/Task (refer to Appendix D) SET shall provide to the DGA a Systems Engineering Management Plan (SEMP) as described in Appendix D.4 “SEMP Annotated Outline” of NPR 7123.1, NASA Systems Engineering Processes and Requirements.”
002	2.2.1	Each Class 3 and Class 4 Program/Project/Task SET shall provide to the DGA the documentation of the material typically found in a SEMP (see Appendix D.4 “SEMP Annotated Outline” of NPR 7123.1) in the manner and form agreed to with the DGA.
003	2.2.4	Each Program/Project/Task SET shall update the SEMP (or alternate documentation as required in Req. 002), prior to each Program/Project/Task lifecycle review.
004	2.2.4	The DGA shall review and approve or disapprove the SEMP (or alternate documentation as required in Req. 002) at each Program/Project/Task lifecycle review.
005	2.3.1	Each Class 1, and 2 Program/Project/Task SET shall follow the best practices enumerated in Appendix E.2 for each of the 17 Common Technical Processes unless the SEMP documents reason(s) for not following particular practice(s).
006	4.1	The PM of the Program/Project/Task shall provide any waiver requests to the LaRC Center Director (or designee) in writing, signed by the PM, and accompanied by evidence of concurrence by the relevant Project Chief Engineer or the Project Lead Systems Engineer and the Program/Project/Task sponsor (the Principal Investigator or other appropriate person).
007	4.2	The PM of the Program/Project/Task shall maintain all waiver documentation.

APPENDIX D. CLASS OF PROGRAM/PROJECT/TASK

D.1 LaRC has established four classes of programs, projects, and tasks, where Class 1 is considered the highest class and Class 4 is considered the lowest class. The classification is done at program/project/task initiation and is reassessed at least annually to determine if the classification should be modified.

D.2 Agency-level Programs and Projects (those identified in the NASA Meta Data Manager database at: https://nsminfo.nasa.gov/nsminfo/home/Disclaimer.aspx) are Class 1. Other Programs/Projects/Tasks are initially classified at the highest level corresponding to planned annual and life-cycle costs (LCC) as indicated in Table D-1. For instance, a Program/Project/Task that is expected to have a LCC of $3M, with annual costs of $1M in the first year and $2M in the second year, would be initially considered as Class 2. Similarly, a Program/Project/Task with an expected annual cost of $1M per year for each of 5 years would also initially be considered as Class 2. For each program/project/task, the DGA according to the initial classification communicates the initial classification to the DGA of the next higher level of classification. The DGA of the higher level (or the Class 1 DGA where there is no higher level) decides whether other factors warrant a change in the initial classification.

D.3 The DGA for Class 1 Programs/Projects/Tasks is the Chair of the LaRC Center Management Council (CMC), or designee. The DGA for Class 2 and Class 3 Programs/Projects/Tasks is the LaRC Chief Engineer or designee. The DGA for Class 4 Programs/Projects/Tasks is the Engineering Director or designee of the organization leading the technical effort of the LaRC portion of the Program/Project/Task.

Class	Annual Cost	And/Or	Life-cycle Cost
1	≥$10M	OR	≥$25M
2	≥$2M and <$10M	OR	≥$5M and <$25M
3	≥$250K and <$2M	OR	≥$1 and <$5M
4	<$250K	AND	<$1M

Table D-1

D.4 Occasionally, LaRC will be responsible for multiple separate systems, subsystems, or elements that are part of a larger final project. For instance, in Figure D-1, the total LaRC portion of the work for the NASA project comprises Element A and Element B. In such cases, the Program/Project/Task class is determined by the total LaRC portion. At the option of the person who would be the DGA of the total LaRC portion, the requirements of this LPR (e.g., SEMP, technical processes) may be met at the level of the total LaRC portion, at the Element A and Element B levels, or both.

D.5 In the example given in Figure D-1, the total LaRC portion has a LCC of $26M, making it a Class 1 Program/Project/Task. At the discretion of the Class 1 DGA, the requirements of this LPR may be met by the PM and SET of the total LaRC portion satisfying the requirements of a Class 1 Program/Project/Task. Alternatively, the Class 1 DGA may decide that the requirements of this LPR are to be met by the PM and SET

of Element A satisfying the requirements of a Class 3 Program/Project/Task and the PM and SET of Element B satisfying the requirements of a Class 2 Program/Project/Task. The Class 1 DGA may also decide that the requirements of this LPR are to be satisfied by both alternatives.

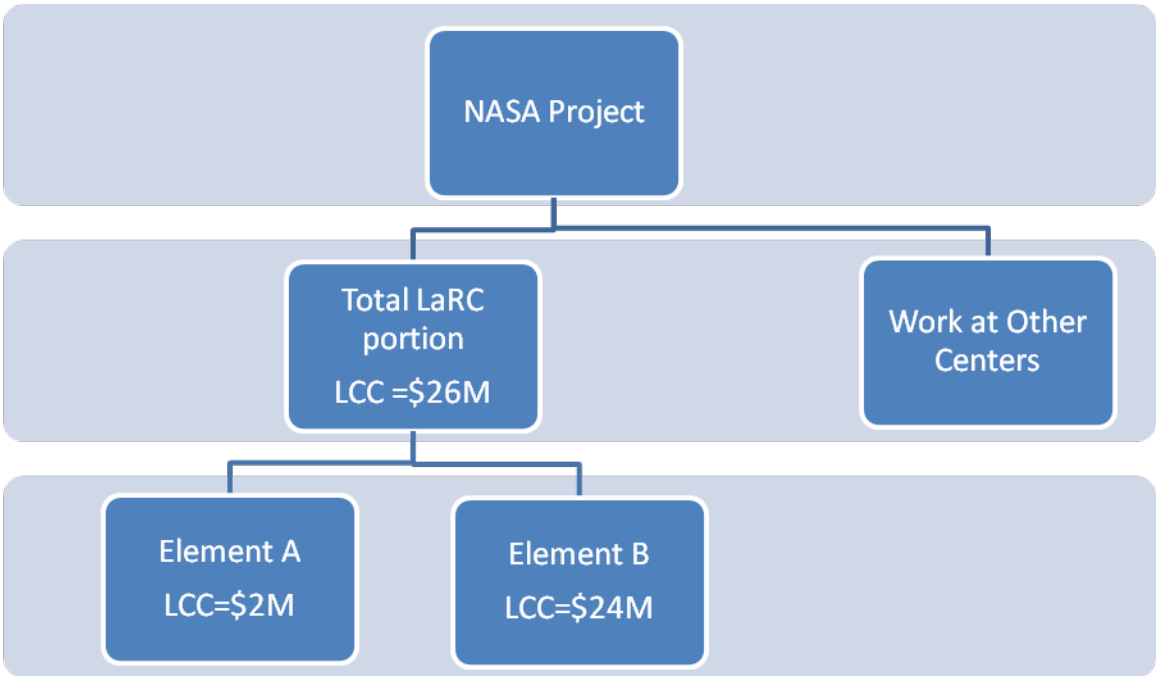


Figure D- 1

APPENDIX E. COMMON TECHNICAL PROCESSES BEST PRACTICES

E.1 Overview

E.1.1 There are one hundred five (105) “Expected Process Activities” presented as the third column of NPR 7123.1 Table 3-1 entitled “Process Activity Traceability Matrix” (pp.H2-2). These activities are considered “Best Practices.” These best practices are extracted from industry, national, international, and agency standards. They provide the best typical practices currently available. These best practices are reformatted and restated in Section E.2 of this appendix to include the addition of a number of LaRC practices that are appropriate to some of the processes. Therefore, while the process numbering is consistent with NPR 7123.1, the numbering of the separate practices is changed to accommodate the LaRC practices.

E.1.2 The 17 common technical processes are enumerated according to their description in this document and their interactions shown in Figure E-1. This SE common technical processes model illustrates the use of: (1) the system design processes for “top down” design of each product in the system structure, (2) the product realization processes for “bottom up” realization of each product in the system structure, and (3) the technical management processes for planning, assessing, and controlling the implementation of the system design and product realization processes and to guide technical decision making (decision analysis). The SE common technical processes model is referred to as an “SE engine” to stress that these common technical processes are used to drive the development of the system products and associated work products required by management to satisfy the applicable product-line life-cycle phase exit criteria while meeting stakeholder expectations within cost, schedule, and risk constraints.

E.1.3 The common technical processes are applied to a product-based Work Breakdown Structure (WBS) model. The processes are used to develop both the products that will satisfy the operational or mission functions of the system (end products) and those that will satisfy the life-cycle support functions of the system (enabling products). The enabling products facilitate the activities of system design, product realization, operations and mission support, sustainment, and end-of-product-life disposal or recycling by having the products and services available when needed.

E.1.4 Langley Form LF-464 can be used as a checklist to track compliance of the practices enumerated in section E.2. The practice description is significantly abbreviated in the form. The full text in section E.2 should be used for a more complete description of each practice.

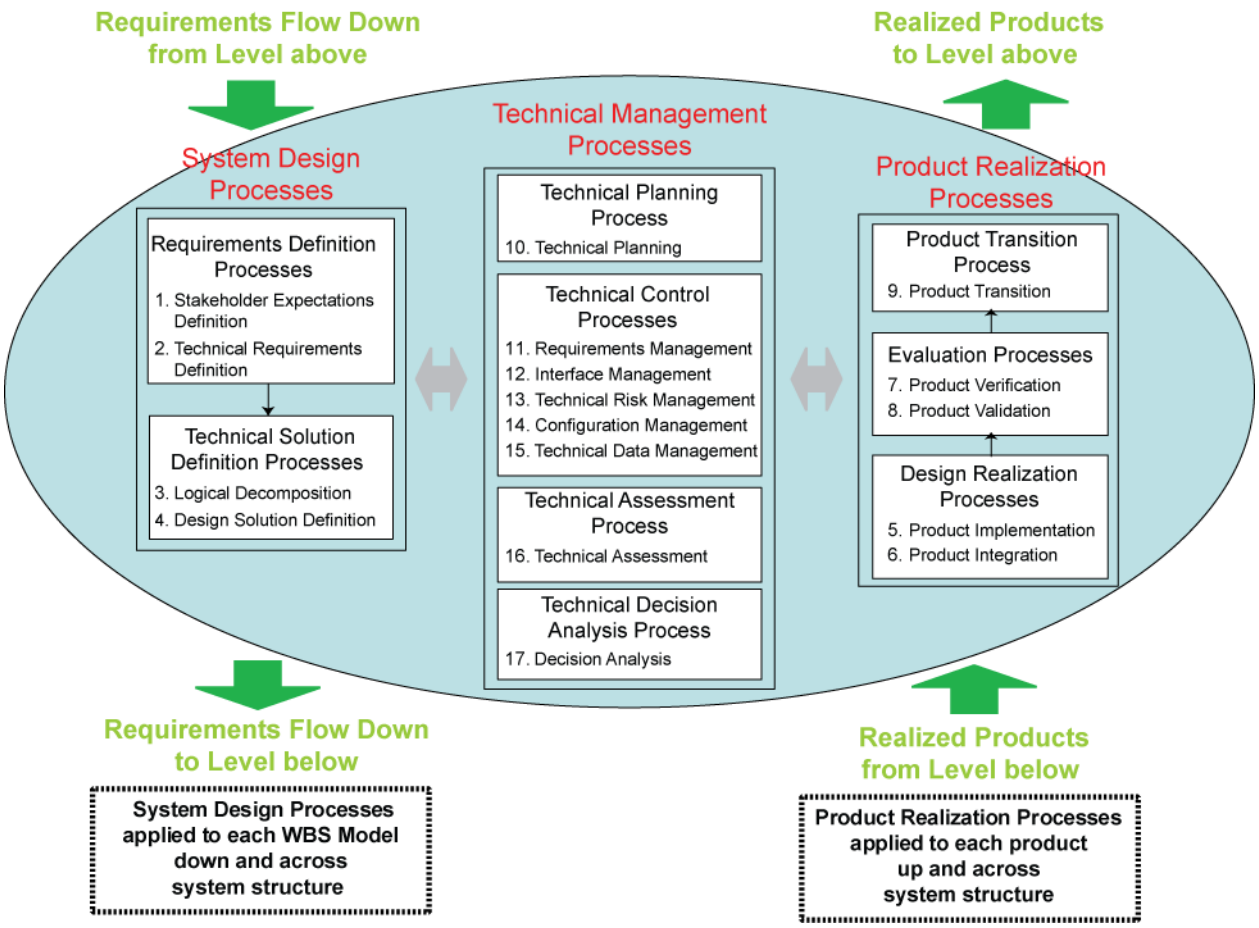


Figure E-1 Systems Engineering Engine

E.2 Systems Engineering Common Technical Processes

E.2.1 Stakeholder Expectations Definition Process Best Practices

E.2.1.1 Establish a list that identifies customers and other stakeholders that have an interest in the system and its products (**NOTE:** *This list should include personnel from the Langley organizations that will be supporting the project, industry partners, Customer engineering and program personnel. The Systems Engineer is advised to include a broad range of technical, program and customer personnel in the discovery of the stakeholders and their needs.*).

E.2.1.2 Elicit customer and other stakeholder expectations (needs, wants, desires, capabilities, external interfaces, and constraints) from the identified stakeholders (*the format in which these inputs are captured conforms to LMS-CP-5526)*.

E.2.1.3 Identify and document all external interfaces (e.g., hardware, software, other systems) for the product. The external interfaces form the boundaries between the system of interest and other systems. If helpful, create, use, and maintain interface diagrams to depict all of the external interfaces. *(This is a LaRC additional practice.)*

E.2.1.4 Validate the customer(s) and other stakeholder expectations and identified external interfaces to ensure all expectations and interfaces are identified and agreed upon. *(This is a LaRC additional practice.)*

E.2.1.5 Establish and then validate operational concepts and support strategies based on stakeholder's expected use of the system products over the system's life, including Assembly, Integration, Test, Transportation, Operations, and Disposal. *(This practice includes LaRC supplementary provisions.)*

E.2.1.6 Define Stakeholder expectations in acceptable statements that are complete sentences and have the following characteristics: (1) individually clear, correct, and feasible to satisfy; implementable; only one interpretation of meaning; one actor-verb-object expectation; and can be validated at the level of the system structure at which it is stated; and (2) in pairs or as a set there is an absence of redundancy, there is consistency with respect to terms used, they are not in conflict with one another, and they do not contain stakeholder expectation of questionable utility or which have an unacceptable risk of satisfaction (**NOTE:** The output of this definition conforms to LMS-CP-5526).

E.2.1.7 Analyze stakeholder expectation statements to establish a set of MOEs by which overall system or product effectiveness will be judged, and customer satisfaction will be determined.

E.2.1.8 Validate that the resulting set of stakeholder expectation statements are upward and downward traceable to reflect the elicited set of stakeholder expectations and that any anomalies identified are resolved.

E.2.1.9 Obtain commitments from customer and other stakeholders that the resultant set of stakeholder expectation statements is acceptable.

E.2.1.10 Baseline the agreed to set of stakeholder expectation statements.

E.2.2 Technical Requirements Definition Process Best Practices

E.2.2.1 Analyze the scope of the technical problem to be solved to identify and resolve the design boundary that identifies: (1) which system functions are under design control and which are not; (2) expected interaction among system functions (data flows, human responses, and behaviors); (3) external physical and functional interfaces (mechanical, electrical, thermal, data, procedural) with other systems; (4) required capacities of system products; (5) timing of events, states, modes, and functions related to operational scenarios; and (6) emerging or maturing technologies necessary to make requirements.

E.2.2.2 Define constraints affecting the design of the system or products or how the system or products will be able to be used.

E.2.2.3 Define functional and behavioral expectations for the system or product in technical terms for the range of anticipated uses of system products as identified in the concept of operations; this permits separating defined stakeholder expectation functions and behaviors that belong to a lower level in the system structure and allocating them to the appropriate level.

E.2.2.4 Define the performance requirements associated with each defined functional and behavioral expectation.

E.2.2.5 Define technical requirements in "shall" statements that are complete sentences with a single "shall" per numbered statement and have the following characteristics: (1) individually clear, correct, and feasible; not stated as to how it is to be satisfied; implementable; only one interpretation of meaning; one actor-verb-object requirement; and can be validated at the level of the system structure at which it is stated; and (2) in pairs or as a set, there is an absence of redundancy, consistency with terms used, no conflict with one another, and form a set of "design-to" requirements.

E2.2.6 Document the rationale (e.g., why requirement exists, assumptions, expected operations, trade study results) for each requirement established. *(This is a LaRC additional practice.)*

E.2.2.7 Validate that the resulting technical requirement statements: (1) have bidirectional traceability to the baselined stakeholder expectations; (2) were formed using valid assumptions; and (3) are essential to and consistent with designing and realizing the appropriate product solution form that will satisfy the applicable product-line life-cycle phase exit criteria.

E.2.2.8 Define MOPs for each identified measure of effectiveness (MOE) that cannot be directly used as a design-to technical requirement.

E.2.2.9 Document the verification method(s), e.g., test, analysis, inspection, demonstration, for each requirement established. *(This is a LaRC additional practice.)*

E.2.2.10 Define appropriate TPMs by which technical progress will be assessed.

E.2.2.11 Establish the technical requirements baseline.

E.2.3 Logical Decomposition Process Best Practices

E.2.3.1 Define one or more logical decomposition models based on the defined technical requirements to gain a more detailed understanding and definition of the design problem to be solved.

E.2.3.2 Allocate the technical requirements to the logical decomposition models to form a set of derived technical requirement statements that have the following

characteristics: (1) describe functional and performance requirements, service and attribute requirements, timing requirements, data flow requirements, and other requirements as appropriate for the selected set of logical decomposition models; (2) individually are complete sentences and are clear, correct, and feasible; not stated as to how to be satisfied; implementable; only have one interpretation of meaning, one actor-verb-object expectation; and can be validated at the level of the system structure at which it is stated; (3) in pairs or as a set, have an absence of redundancy, are adequately related with respect to terms used, and are not in conflict with one another; and (4) form a set of detailed "design-to" requirements.

E.2.3.3 Resolve derived technical requirement conflicts.

E.2.3.4 Validate that the resulting set of derived technical requirements have: (1) bidirectional traceability with the set of validated technical requirements and (2) assumptions and decision rationales consistent with the source set of technical requirements.

E.2.3.5 Validate the resultant set of requirements to ensure stakeholders agree that the requirements have been identified and allocated to the appropriate models (e.g., elements and subsystems) and baseline this set of requirements. *(This is a LaRC additional practice.)*

E.2.3.6 Establish the derived technical requirements baseline.

E.2.4 Design Solution Definition Process Best Practices

E.2.4.1 Define alternative solutions for the system end product being developed or improved that are consistent with derived technical requirements and non-allocated technical requirements, if any.

E.2.4.2 Analyze each alternative solution against defined criteria, such as satisfaction of external interface requirements; technology requirements; off-the-shelf availability of products; physical failure modes, effects, and criticality; life-cycle cost and support considerations; capacity to evolve; make vs. buy; standardization of products; integration concerns; and context of use issues of operators considering tasks, location, workplace equipment, and ambient conditions.

E.2.4.3 Select the best solution alternative based on the analysis results of each alternative solution and technical decision analysis recommendations.

E.2.4.4 Generate the full design description of the selected alternative solution in a form appropriate to the product-line life-cycle phase, location of the WBS model in the system structure, and phase exit criteria to include: (1) system specification and external interface specifications; (2) end product specifications, configuration description documents, and interface specifications; (3) end product subsystem initial specifications, if subsystems are required; (4) requirements for associated supporting

enabling products; (5) end product verification plan; (6) end product validation plan; and (7) applicable logistics and operate-to procedures.

E.2.4.5 Verify that the design solution definition: (1) is realizable within constraints imposed on the technical effort; (2) has specified requirements that are stated in acceptable statements and have bidirectional traceability with the derived technical requirements, technical requirements, and stakeholder expectations; and (3) has decisions and assumptions made in forming the solution consistent with its set of derived technical requirements, separately allocated technical requirements, and identified system product and service constraints.

E.2.4.6 Baseline the design solution definition specified requirements including the specifications and configuration descriptions.

E.2.4.7 Initiate development or acquisition of the life-cycle supporting enabling products needed, as applicable, for research, development, fabrication, integration, test, deployment, operations, sustainment, and disposal.

E.2.4.8 Initiate development of the system products of the next lower level WBS model, if any.

E.2.5 Product Implementation Process Best Practices

E.2.5.1 Prepare to conduct product implementation including: (1) prepare a product implementation strategy and detailed planning and procedures and (2) determine whether the product configuration documentation is adequately complete to conduct the type of product implementation as applicable for the product-line life-cycle phase, location of the product in the system structure, and phase exit criteria.

E.2.5.2 If the strategy is for buying an existing product, participate in the buy of the product including: (1) review the technical information made available by vendors; (2) assist the preparation of requests for acquiring the product from a vendor; (3) assist the inspection of the delivered product and the accompanying documentation; (4) determine whether the vendor conducted product validation or if it will need to be done by a project technical team; and (5) determine the availability of enabling products to provide test, operations, and maintenance support and disposal services for the product.

E.2.5.3 If the strategy is to reuse a product that exists in the Government inventory, participate in acquiring the reused product including: (1) review the technical information made available for the specified product to be reused; (2) determine supporting documentation and user manuals availability; (3) determine the availability of enabling products to provide test, operations, and maintenance support and disposal services for the product; (4) assist the requests for acquiring the product from Government sources; and (5) assist the inspection of the delivered product and the accompanying documentation.

E.2.5.4 If the strategy is to make the product: (1) evaluate the readiness of the product implementation enabling products to make the product, (2) make the specified product in accordance with the specified requirements, configuration documentation, and applicable standards, and (3) prepare appropriate product support documentation, such as integration constraints and/or special procedures for performing product verification and product validation.

E.2.5.5 Capture work products and related information generated while performing the product implementation process activities.

E.2.5.6 Abide by any relevant requirements identified in the *Procurement Initiator's Guide* (LPR 5000.2). *(This is a LaRC additional practice.)*

E.2.6 Product Integration Process Best Practices

E.2.6.1 Prepare to conduct product integration to include: (1) preparing a product integration strategy, detailed planning for the integration, and integration sequences and procedures; and (2) determining whether the product configuration documentation is adequately complete to conduct the type of product integration applicable for the product-line life-cycle phase, location of the product in the system structure, and management phase exit criteria.

E.2.6.2 Document and approve integration procedures and sequences including a "completion timeline" that supports the "need date". *(This is a LaRC additional practice.)*

E.2.6.3 Obtain lower level products required to assemble and integrate into the desired product.

E.2.6.4 Confirm received products being integrated have been verified to their own specific set of requirements. *(This is a LaRC additional practice.)*

E.2.6.5 Confirm that the received products that are to be assembled and integrated have been validated to demonstrate that the individual products satisfy the agreed upon set of stakeholder expectations, including interface requirements.

E.2.6.6 Prepare the integration environment in which assembly and integration will take place to include evaluating the readiness of the product-integration enabling products and the assigned workforce.

E.2.6.7 Assemble and integrate the received products into the desired end product in accordance with the specified requirements, configuration documentation, interface requirements, applicable standards, and integration sequencing and procedures.

E.2.6.8 Document results/modifications/changes generated during integration. *(This is a LaRC additional practice.)*

E.2.6.9 Prepare appropriate product support documentation, such as special procedures for performing product verification and product validation.

E.2.6.10 Document delivery of the end product for higher level processing. *(This is a LaRC additional practice.)*

E.2.6.11 Capture work products and related information generated while performing the product integration process activities.

E.2.7 Product Verification Process Best Practices

E.2.7.1 Prepare to conduct product verification to include as applicable to the product-line life-cycle phase and WBS model location in the system structure: (1) reviewing the product verification plan for specific procedures, constraints, conditions under which verification will take place, pre- and post-verification actions, and criteria for determining the success or failure of verification methods and procedures; (2) arranging the needed product-verification enabling products and support resources; (3) obtaining the end product to be verified; (4) obtaining the specification and configuration baseline against which the verification is to be made; and (5) establishing and checking the verification environment to ensure readiness for performing the verification.

E.2.7.2 Perform the product verification in accordance with the product verification plan and defined procedures to collect data on each specified requirement with specific attention given to MOPs.

E.2.7.3 Analyze the outcomes of the product verification, including identifying verification anomalies, establishing recommended corrective actions, and establishing conformance to each specified requirement under controlled conditions.

E.2.7.4 Prepare a product verification report providing the evidence of product conformance with the applicable design solution definition specified requirements baseline to which the product was generated, including bidirectional requirements traceability and actions taken to correct anomalies of verification results.

E.2.7.5 Capture the work products from the product verification.

E.2.8 Product Validation Process Best Practices

E.2.8.1 Prepare to conduct product validation to include as applicable to the product-line life-cycle phase and product location in the system structure: (1) reviewing the product validation plan for specific procedures, constraints, conditions under which validation will take place, pre- and post-validation actions, and criteria for determining the success or failure of validation methods and procedures; (2) arranging the needed product-validation enabling products and support resources; (3) obtaining the end product to be validated; (4) obtaining the stakeholder expectations baseline against which the validation is to be made; and (5) establishing and evaluating the validation environment to ensure readiness for performing the validation.

E.2.8.2 Perform the product validation in accordance with the product validation plan and defined procedures to collect data on performance of the product against stakeholder expectations with specific attention given to MOEs.

E.2.8.3 Analyze the outcomes of the product validation to include identification of validation anomalies, establishing recommended corrective actions, and establishing conformance to stakeholder expectations under operational conditions (actual, analyzed, or simulated).

E.2.8.4 Prepare a product validation report providing the evidence of product conformance with the stakeholder expectations baseline, including corrective actions taken to correct anomalies of validation results.

E.2.8.5 Capture the work products from the product validation.

E.2.9 Product Transition Process Best Practices

E.2.9.1 Prepare to conduct product transition to include: (1) preparing a product implementation strategy to establish the type of product transition to be made (to the next higher level customer for product integration or to an end user); and (2) reviewing related end product stakeholder expectations and design solution definition specified requirements to identify special transition procedures and enabling product needs for the type of product transition, if any, for packaging, storage, handling, shipping/transporting, site preparation, installation, or sustainment.

E.2.9.2 Evaluate the end product, personnel, and enabling product readiness for product transition including: (1) availability and appropriateness of the documentation that will be packaged and shipped with the end product; (2) adequacy of procedures for conducting product transition; (3) availability and skills of personnel to conduct product transition; and (4) availability of packaging materials/containers, handling equipment, storage facilities, and shipping/transporter services.

E.2.9.3 Prepare the end product for transition to include the packaging and moving the product to the shipping/transporting location and any intermediate storage.

E.2.9.4 Transition the end product with required documentation to the customer, based on the type of transition required, e.g., to the next higher level WBS model for product integration or to the end user.

E.2.9.5 Prepare sites, as required, where the end product will be stored, assembled, integrated, installed, used, or maintained, as appropriate for the life-cycle phase, position of the end product in the system structure, and customer agreement.

E.2.9.6 Abide by any relevant requirements identified in *Product Assurance Plan* (LPR 5300.1) and *Handling, Preservation, Storage, and Shipping of Space Flight Hardware* (LMS-CP-4756). *(This is a LaRC additional practice.)*

E.2.9.7 Capture work products from product transition process activities.

E.2.10 Technical Planning Management Process Best Practices

E.2.10.1 Prepare to conduct technical planning to include: (1) preparing or updating a planning strategy for each of the common technical processes and (2) determining:

a. deliverable work products from technical efforts,
b. technical reporting requirements,
c. other technical information needs for reviews or satisfying product-line life-cycle management phase entry or exit criteria,
d. product and process measures to be used in measuring technical performance, cost, and schedule progress,
e. key or critical technical events with entry and success criteria,
f. data management approach for data collection and storage and how measurement data will be analyzed, reported, and dispositioned as Federal records,
g. technical risks that need to be addressed in the planning effort,
h. tools and engineering methods to be employed in the technical effort, and
i. approach to acquiring and maintaining the technical expertise needed (training and skills development plan).

E.2.10.2 Identify and plan for data archiving of LaRC-delivered data products. *(This is a LaRC additional practice.)*

E.2.10.3 Identify and plan for preservation of records in accordance with *Langley Research Center Records Management Procedural* Requirements (LPR 1440.7). *(This is a LaRC additional practice.)*

E.2.10.4 Identify and plan for hardware to be retained and stored, including storage location and requirements (e.g., environmentally controlled storage). *(This is a LaRC additional practice.)*

E.2.10.5 Define the technical work to be done to include associated technical, support, and management tasks needed to generate the deliverable products and satisfy entry and success criteria of key technical events and the applicable product-line life-cycle management phase.

E.2.10.6 Schedule, organize, and determine the cost of the technical effort.

E.2.10.7 Prepare the SEMP and other technical plans needed to support the technical effort and perform the technical processes.

E.2.10.8 Obtain stakeholder commitments to the technical plans.

E.2.10.9 Issue authorized technical work directives to implement the technical work.

E.2.10.10 Capture work products from technical planning activities.

E.2.11 Technical Requirements Management Process Best Practices

E.2.11.1 Prepare to conduct requirements management to include: (1) preparing or updating a strategy and procedures for: (a) establishing that expectation and requirement statements, singularly and as a whole, are prepared in accordance with established formats and rules; (b) identifying expectations and requirements to be managed, expectation and requirement sources, and allocation and traceability of requirements and linking product expectations and requirements with costs, weight, and power allocations, as applicable; and (c) formal initiation, assessment, review, approval, and disposition of engineering change proposals and changes to expectation and requirements baseline; (2) selecting or updating an appropriate requirements management tool; and (3) training technical team members in the established requirements management procedures and in the use of the selected/updated requirements management tool.

E.2.11.2 Conduct requirements management to include: (1) capturing, storing, and documenting the expectations and requirements; (2) establishing that expectation and requirement statements are compliant with format and other established rules (e.g., LMS-CP-5526); (3) confirming each established requirements baseline has been validated; and (4) identifying and analyzing out-of-tolerance system-critical technical parameters and unacceptable validation and verification results and proposing requirement-appropriate changes to correct out-of-tolerance requirements. *(This practice has been modified with supplementary LaRC material.)*

E.2.11.3 Conduct expectation and requirements traceability to include: (1) tracking expectations and requirements between baselines, especially MOEs, MOPs, and TPMs and (2) establishing and maintaining appropriate requirements compliance matrixes that contain the requirements, bidirectional traceability, compliance status, and any actions to complete compliance.

E.2.11.4 Manage expectation and requirement changes to include: (1) reviewing engineering change proposals (ECPs) to determine any changes to established requirement baselines; (2) documenting requested requirement(s) change (e.g., modification, addition, or deletion) with justification for change; (3) communicating the requested requirement(s) change to all stakeholders who are impacted; (4) ensuring that each requested requirement(s) change includes an evaluation of the impact (e.g., cost, schedule, technical, higher/derived/lower/interface requirements, effect on constituent parts, components and products already delivered) of the requested requirement(s) change; (5) implementing formal change procedures for proposed and identified expectation or requirement changes; and (6) disseminating the approved change information. *(This practice has been modified with supplementary LaRC material.)*

E.2.11.5 Capture work products from requirements management process activities to include maintaining and reporting information on the rationale for and disposition and implementation of change actions, current requirement compliance status, and expectation and requirement baselines.

E.2.12 Technical Interface Management Process Best Practices

E.2.12.1 Prepare or update interface management procedures for: (1) establishing interface management responsibilities for those interfaces that are part of agreement boundaries; (2) maintaining and controlling identified internal and external physical and functional interfaces; (3) preparing and maintaining appropriate physical and functional interface specifications or interface control documents and drawings to describe and control interfaces external to the system end product; (4) identifying interfaces between system products (including humans) and among configuration management items; (5) establishing and implementing formal change procedures for interface evolution; (6) disseminating the needed interface information for integration into technical effort activities and for external interface control; and (7) training technical teams and other applicable support and management personnel in the established interface management procedures.

E.2.12.2 Conduct interface management during system design activities for each WBS model in the system structure to include: (1) integrating the interface management activities with requirements management activities; (2) analyzing the concept of operations to identify critical interfaces not included in the stakeholder set of expectations; (3) documenting interfaces both external and internal to each WBS model as the development of the system structure emerges and interfaces are added and existing interfaces are changed; (4) documenting origin, destination, stimulus, and special characteristics of interfaces; (5) maintaining the design solution definition for internal horizontal and vertical interfaces between WBS models in the system structure; (6) maintaining horizontal traceability of interface requirements across interfaces and capturing status in the established requirements compliance matrix; and (7) confirming that each interface control document or drawing that is established has been validated with parties on both sides of the interface.

E.2.12.3 Conduct interface management during product integration activities to include: (1) reviewing product integration procedures to ensure that interfaces are marked to ensure easy and correct assembly/connection with other products; (2) identifying product integration planning to identify interface discrepancies, if any, and report to the proper technical team or technical manager; (3) confirming that a check is completed on all physical interfaces before connecting products; (4) evaluating assembled products for interface compatibility; (5) confirming that product verification and product validation plans/procedures include confirming internal and external interfaces; and (6) preparing an interface evaluation report upon completion of integration, product verification, and product validation.

E.2.12.4 Conduct interface control to include: (1) managing interface changes within the system structure; (2) identifying and tracking proposed and directed changes to

interface specifications and interface control documents and drawings; (3) confirming that the vertical and horizontal interface issues are analyzed and resolved when a change affects products on both sides of the interface; (4) controlling traceability of interface changes including source of the change, processing methods, and approvals; and (5) disseminating the approved interface change information for integration into technical efforts at every level of the project.

E.2.12.5 Capture work products from interface management activities.

E.2.13 Technical Risk Management Process Best Practices

E.2.13.1 Prepare a strategy to conduct technical risk management to include: (1) documenting how the project risk management plan will be implemented in the technical effort; (2) planning identification of technical risk sources and categories; (3) identification of potential technical risks; (4) characterizing and prioritizing technical risks; (5) planning informed technical management (mitigation) actions should the risk event occur; (6) tracking technical risk status against established triggers; (7) resolving technical risk by taking planned action if established triggers are tripped; and (8) communicating technical risk status and mitigation actions taken, when appropriate.

E.2.13.2 Identify technical risks to include: (1) identifying sources of risk issues related to the technical effort; (2) anticipate what could go wrong in each of the source areas to create technical risk issues; (3) analyzing identified technical risks for cause and importance; (4) preparing clear, understandable, and standard form risk statements; and (5) coordinating with relevant stakeholders associated with each identified technical risk.

E.2.13.3 Conduct technical risk assessment to include: (1) categorize the severity of consequences for each identified technical risk in terms of performance, cost, and schedule impacts to the technical effort and project; (2) analyze the likelihood and uncertainties of events associated with each technical risk and quantify (for example, by probabilities) or qualify (for example, by high, moderate, or low) the probability of occurrence in accordance with project risk management plan rules; and (3) prioritize risks for mitigation.

E.2.13.4 Prepare for technical risk mitigation to include: (1) selecting risks for mitigation and monitoring; (2) selecting an appropriate risk-handling approach; (3) establishing the risk level or threshold when risk occurrence becomes unacceptable and triggers execution of a risk mitigation action plan; (4) selecting contingency actions and triggers should risk mitigation not work to prevent a problem occurrence; (5) preparing risk mitigation and contingency action plans identifying responsibilities and authorities.

E.2.13.5 Monitor the status of each technical risk periodically to include: (1) tracking risk status to determine whether conditions or situations have changed so that risk monitoring is no longer needed or new risks have been discovered; (2) comparing risk status and risk thresholds; (3) reporting risk status to decision authorities when a threshold has been triggered and an action plan implemented; (4) preparing technical

risk status reports as required by the project risk management plan; (5) communicating risk status during technical reviews in the form specified by the project risk management plan.

E.2.13.6 Implement technical risk mitigation and contingency action plans when the applicable thresholds have been triggered to include: (1) monitoring the results of the action plan implemented; (2) modifying the action plan as appropriate to the results of the actions; (3) continuing actions until the residual risk and/or consequences impacts are acceptable or become a problem to be solved; (4) communicate to the project when risks are beyond the scope of the technical effort to control, will affect a product higher in the system structure, or represent a significant threat to the technical effort or project success; (5) preparing action plan effectiveness reports as required by the project risk management plan; (6) communicating action plan effectiveness during technical reviews in the form specified by the project risk management plan.

E.2.13.7 Abide by the appropriate additional requirements identified in *Product Assurance Plan* (LPR 5300.1) Section 4.1.2, Risk Management Requirements. *(This is a LaRC additional practice.)*

E.2.13.8 Capture work products from technical risk management activities.

E.2.14 Technical Configuration Management Process Best Practices

E.2.14.1 Prepare a strategy to conduct configuration management for the system products and designated work products to include: (1) documenting how the project configuration management plan, if any, will be implemented; (2) identifying items to be put under configuration control; (3) identifying schema of identifiers to accurately describe a configuration item and its revisions or versions; (4) controlling changes to configuration items; (5) maintaining and reporting disposition and implementation of change actions to appropriate stakeholders including technical teams within the project; (6) ensuring that products are in compliance with specifications and configuration documentation during reviews and audits; (7) providing the appropriate reference configuration at the start of each product-line life-cycle phase; (8) obtaining appropriate tools for configuration management; and (9) training appropriate technical team members and other technical support and management personnel in the established configuration management strategy and any configuration management procedures and tools.

E.2.14.2 Identify baselines to be under configuration control to include: (1) listing of the configuration items to control; (2) providing each configuration item with a unique identifier; (3) identifying acceptance requirements for each baseline identified for control; (4) identifying the owner of each configuration item; and (5) establishing a baseline configuration for each configuration item.

E.2.14.3 Manage configuration change control to include: (1) establishing change criteria, procedures, and responsibilities; (2) receiving, recording, and evaluating change requests; (3) tracking change requests to closure; (4) obtaining appropriate

approvals before implementing a change; (5) incorporating approved changes in appropriate configuration items; (6) releasing changed configuration items for use; and (7) monitoring implementation to determine whether changes resulted in unintended effects (e.g., have compromised safety or security of baseline product).

E.2.14.4 Maintain the status of configuration documentation to include: (1) maintaining configuration item description records and records that verify readiness of configuration items for testing, delivery, or other related technical efforts; (2) maintaining change requests, disposition action taken, and history of change status; (3) maintaining differences between successive baselines; and (4) controlling access to and release of configuration baselines.

E.2.14.5 Conduct configuration audits to include: (1) auditing baselines under control to confirm that the actual work product configuration matches the documented configuration, the configuration is in conformance with product requirements, and records of all change actions are complete and up to date; (2) identifying risks to the technical effort based on incorrect documentation, implementation, or tracking of changes; (3) assessing the integrity of the baselines; (4) confirming the completeness and correctness of the content of configuration items with applicable requirements; (5) confirming compliance of configuration items with applicable configuration management standards and procedures; and (6) tracking action items to correct anomalies from audit to closure.

E.2.14.6 Abide by the appropriate additional requirements identified in *Flight Projects Directorate Space Flight Configuration Management Requirements* (LPR 8040.1). *(This is a LaRC additional practice.)*

E.2.14.7 Capture work products from configuration management activities to include: (1) a list of identified configuration items; (2) description of configuration items placed under control; (3) change requests, disposition of the requests, and rationale for the dispositions; (4) documented changes with reason for changes and change actions; (5) archive of old baselines; and (6) required reports on configuration management outcomes.

E.2.15 Technical Data Management Process Best Practices

E.2.15.1 Prepare a strategy for the conduct of technical data management to include: (1) determining required data content and form and electronic data exchange interfaces in accordance with international standards or agreements; (2) establishing a framework for technical data flow within the project technical processes and to/from contractors; (3) designating technical data management responsibilities and authorities regarding origination, generation, capture, archiving, security, privacy, and disposal of technical data work products; (4) establishing the rights, obligations and commitments regarding the retention of, transmission of, and access to technical data items; (5) establishing relevant data storage, transformation, transmission and presentation standards and conventions to be used; (6) establishing project or program policy and agreements or legislative constraints; (7) describing the methods, tools, and metrics used during the

technical effort and for technical data management; and (8) training appropriate technical team members and support and management personnel in the established technical data management strategy and related procedures and tools.

E.2.15.2 Collect and store required technical data to include: (1) identifying existing sources of technical data that are designated as outputs of the common technical processes; (2) collecting and storing technical data in accordance with the technical data management strategy and procedures; (3) recording and distributing lessons learned; (4) performing technical data integrity checks on collected data to confirm compliance with content and format requirements and identifying errors in specifying or recording data; and (5) prioritizing, reviewing, and updating technical data collection and storage procedures.

E.2.15.3 Maintain stored technical data to include: (1) managing the databases to maintain proper quality and integrity of the collected and stored technical data and to confirm that the technical data is secure and is available to those with authority to have access; (2) performing technical data maintenance as required; (3) preventing the stored data from being used or accessed inappropriately; (4) maintaining the stored technical data in a manner that protects it against foreseeable hazards, such as fire, flood, earthquake, and riots; and (5) maintaining periodic backups of each technical database.

E.2.15.4 Provide technical data to authorized parties to include: (1) maintaining an information library or reference index to provide data available and access instructions; (2) receiving and evaluating requests for technical data and delivery instructions; (3) confirming that required and requested technical data is appropriately distributed to satisfy the needs of the requesting party and in accordance with established procedures, directives, and agreements; (4) confirming that electronic access rules are followed before allowing access to the database and before any data is electronically released/transferred to the requester; and (5) providing proof of correctness, reliability, and security of technical data provided to internal and external recipients.

E.2.15.5 Abide by the appropriate additional requirements identified in *Space Flight Project Practices Handbook* (LPR 7120.5), *Langley Research Center Records Management Procedural Requirements* (LPR 1440.7), *Export Control* (LMS-CP-1725), and *Electronic Storage and Archival System* (LMS-CP-2310). *(This is a LaRC additional practice.)*

E.2.16 Technical Assessment Process Best Practices

E.2.16.1 Prepare a strategy for conducting technical assessments to include: (1) identifying the plans against which progress and achievement of the technical effort are to be assessed; (2) establishing procedures for obtaining cost expenditures against work planned and task completions against schedule; (3) identifying and obtaining technical requirements against which product development progress and achievement will be assessed and establishing the procedures for conducting the assessments; (4) establishing events when TPMs, estimation or measurement techniques, and rules for taking action when out-of-tolerance conditions exist will be assessed; (5) identifying and planning for phase-to-phase technical reviews and WBS model-to-model vertical progress reviews, as well as establishing review entry and success criteria, review board members, and close out procedures; (6) establishing which technical effort work products will undergo peer review, the team members who will perform the peer reviews, and reporting requirements; and (7) training team members, support staff, and managers involved in conducting technical assessment activities.

E.2.16.2 Assess technical work productivity (progress and achievement against plans) to include: (1) identifying, collecting, and analyzing process measures (e.g., earned value measurements for measuring progress against planned cost, schedule, resource use, and technical effort tasks) and identifying and reporting cost-effective changes to correct variances; (2) monitoring stakeholder involvement according to the SEMP; and (3) monitoring technical data management against plans.

E.2.16.3 Assess product quality (progress and achievements against technical requirements) to include: (1) identifying, collecting, and analyzing the degree of technical requirement and TPM satisfaction; (2) assessing the maturity of the WBS-model products and services as applicable to the product-line life-cycle phases; (3) determining any variances from expected values of product performance and identifying and defining cost-effective changes to correct variances.

E.2.16.4 Conduct technical reviews to include: (1) identifying the type of technical reviews and each review's purpose and objectives; (2) determining progress toward satisfying entry criteria; (3) establishing the makeup of the review team; (4) preparing the review presentation materials; and (5) identifying and resolving action items resulting from the review.

E.2.16.5 Abide by the appropriate additional requirements identified in *Project and Task Review Procedural Requirements* (LPR 7130), *Space Flight Independent Life Cycle Review Procedural Requirements* (LPR 7120.7), *Review Program for Langley Research Center Facility Projects* (LAPD 7000.2). *(This is a LaRC additional practice.)*

E.2.16.6 Capture work products from the conduct of technical assessment activities to include: (1) identifying variances resulting from technical assessments; (2) identifying and reporting changes to correct variances; (3) recording methods used in doing assessment activities; (4) documenting assumptions made in arriving at the process and product measure outcomes; and (5) reporting corrective action recommendations.

E.2.17 Technical Decision Analysis Process Best Practices

E.2.17.1 Establish guidelines to determine which technical issues are subject to a formal analysis/evaluation process to include: (1) when to use a formal decision-making procedure, for example, as a result of an effectiveness assessment, a technical tradeoff, a problem needing to be solved, action needed as a response to risk exceeding the acceptable threshold, verification or validation failure, make-buy choice, evaluating a solution alternative, or resolving a requirements conflict; (2) what needs to be documented; (3) who will be the decision makers and their responsibilities and decision authorities; and (4) how decisions will be handled that do not require a formal evaluation procedure.

E.2.17.2 Define the criteria for evaluating alternative solutions to include: (1) the types of criteria to consider include the following: technology limitations, environmental impact, safety, risks, total ownership and life-cycle costs, and schedule impact; (2) the acceptable range and scale of the criteria; and (3) the rank of each criterion by its importance.

E.2.17.3 Identify alternative solutions to address decision issues to include alternatives for consideration in addition to those that may be provided with the issue.

E.2.17.4 Select evaluation methods and tools/techniques based on the purpose for analyzing a decision and on the availability of the information used to support the method and/or tool.

E.2.17.5 Evaluate alternative solutions with the established criteria and selected methods to include: (1) evaluation of assumptions related to evaluation criteria and of the evidence that supports the assumptions; and (2) evaluation of whether uncertainty in the values for alternative solutions affects the evaluation.

E.2.17.6 Select recommended solutions from the alternatives based on the evaluation criteria to include documenting the information that justifies the recommendations and gives the impacts of taking the recommended course of action.

E.2.17.7 Report the analysis/evaluation results/findings with recommendations, impacts, and corrective actions.

E.2.17.8 Capture work products from decision analysis activities to include: (1) decision analysis guidelines generated and strategy and procedures used; (2) analysis/evaluation approach, criteria, and methods and tools used; (3) analysis/evaluation results, assumptions made in arriving at recommendations, uncertainties and sensitivities of the recommended actions or corrective actions; and (4) lessons learned and recommendations for improving future decision analyses.

APPENDIX F. REFERENCES

The following documents may be useful to individuals in addressing the requirements of this LPR.

a. NPR 1441.1, NASA Records Retention Schedules

b. NASA/SP-2007-6105, NASA Systems Engineering Handbook

c. NPR 8000.4A, Agency Risk Management Procedural Requirements

d. CMMI® Guidelines for Process Integration and Product Improvement – Addison-Wesley

e. LPR 7120.4, LaRC Technical Authority Implementation Plan

APPENDIX G. LARC SPECIFIC ENGINEERING BEST PRACTICES

(See Langley Form LF 209 Langley Engineering Best Practices for an Excel Spreadsheet of this appendix)

Item Number	LaRC-Specific Engineering Best Practices	Common Technical Processes	Source
1.00	**Assembly Integration and Test (AIT)**		
1.01	**AIT - General**		
1.01.01	**Verification Methods Hierarchy -** Testing should be the primary method for design verification. However, selection of verification methods should be based on technical, cost, and schedule risk analysis. Other methods of verification to be considered should include inspections, analysis or demonstrations. Results of verification by analysis using models or simulations should be independently reviewed and should include a validation of the simulation or model to ensure the appropriateness of its use.	E.2.07 Product Verification	LPR 8705, paragraph 2.23.7
1.01.02	**Test As You Fly** - "Test as you fly and fly as you test" (e.g., using flight sequences, flight-like operating conditions, and the same software functionality) needs to be the system verification philosophy. Where testing is not possible, verification should be demonstrated by independent analyses.	E.2.07 Product Verification	LPR 7120.5, paragraph 6.3 GSFC - STD - 1000 Rule 1.09 LPR 8705.1, paragraph 2.23.2
1.01.03	**Qual Testing Expectations** - During qualification testing, hardware should demonstrate expected (i.e.: within-tolerance) performance over a range of conditions that envelops the worst-case operating parameters anticipated to occur during the planned operational mission. Testing at all levels (system, sub-system, and component) should have clearly defined pass/fail criteria.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 1.13

1.01.04	**Ground Support Equipment (GSE) Usage** - All testing of operations of flight systems at the launch site or in the field should only use GSE and test configurations that have been previously used with the flight hardware.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 1.15
1.01.05	**Heritage Items Assessment** - Prior to using inherited items, cognizant engineers and mission assurance personnel should review the complete pedigree of the inherited item. The project should review and justify any differences in the qualification environments from the inheritance to the intended application.	E.2.04 Design Solution Definition	LPR 7120.5, paragraph 6.6.2
1.02	**AIT - System Level Testing**		
1.02.01	**System Alignment Verifications** - System alignment verifications should be performed before and after exposure to system environmental testing.	E.2.07 Product Verification	JPL D-17868, paragraph 8.3.3.6
1.02.02	**Functional Performance Verification** - Functional performance verifications should be performed before and after exposure to system environmental testing.		
1.02.03	**Spacecraft (S/C) - Launch Vehicle (L/V) Interface Verification** - Early verification of the mechanical interface between the spacecraft and launch vehicle should be performed using an identical mechanical mock-up sufficiently in advance of integrated operations to be able to recover from any unexpected incompatibility.	E.2.07 Product Verification	JPL D-17868, paragraph 8.3.8.1
1.02.04	**System End-to-End Test** - System end-to-end testing should be performed using actual hardware or emulation, and should apply from input to instrument(s), through the spacecraft, transmitted to receiving antennas, and through the ground system - reconciled against what is physically achievable before launch, and consistent with associated mission risk.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 1.08

1.02.05	**Mechanical Environmental Testing** - Mechanical environmental testing (sine, random & acoustic) of flight hardware should be performed with the test article in appropriate (e.g. launch, landing, etc.) configuration. Hardware that is to be powered on for launch should be powered on for testing.	E.2.08 Product Validation	GSFC - STD - 1000 Rule 4.11
1.02.06	**Unique Launch Site Operations** - Unique operations and procedures to be used at the launch site should be dry run before shipment of the flight system to the launch site.	E.2.08 Product Validation	JPL D-17868, paragraph 8.2.3
1.02.07	**Launch Site Testing of Flight System** - The flight system should be functionally tested after delivery to the launch site and prior to mating with the launch vehicle.	E.2.08 Product Validation	JPL D-17868, paragraph 8.4.1.1
1.03	**AIT - Models and Test Beds**		
1.03.01	**Early Identification of Test Beds** - The number and type of test beds, including software-only test beds, and ground support equipment (hardware and software) should be identified and provided early in the development plan.	E.2.07 Product Verification	LPR 8705.1, paragraph 2.20.1
1.03.02	**Test Bed Supporting Orbital Operations** - Develop a test bed (spread system) to verify flight software changes and support troubleshooting activities during orbital operations. Ideally the test bed should have near flight-like fidelity and employ test hardware and software used during the development phase.	E.2.07 Product Verification	LPR 8705.1, paragraph 2.20.3
2.00	**Command & Data Handling (C&DH) -** Also see section 4.04 - Electronic Systems - Telemetry		

2.01	**C&DH - General**		
2.01.01	**Use of data editing, data compression** - To minimize down link telemetry, the information system design should use wherever possible, data editing, data averaging, data compression, and improved data encoding techniques to meet downlink telemetry data requirements. - Also see 7.01.01 - Operations - General	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.8.2
2.01.02	**Minimum number of normal-operations data modes** The information system design should use the *minimum* number of normal-operations data modes to meet the science/engineering requirements. Acceptable sub-optimum return should be considered, particularly if cost/risk can be significantly reduced. Also see 7.01.06 - Operations - General.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.8.4
2.01.03	**Emergency data modes** The information system design should have engineering emergency data modes and formats (measurements) for diagnostic use. A hierarchical measurement approach should be used so that assessment of spacecraft/payload/instrument health/safety can be rapidly attained.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.8.6
2.01.04	**Assessing Health Status** The information system design should provide adequate telemetry data to rapidly assess health status under *normal and faulted* operations. Special consideration should be given to providing increased telemetry instrumentation for mission-unique or other sensitive functions.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.8.7
2.01.05	**Data for Anomaly Determination** - The information system design should provide sufficient telemetry data and sampling frequency, including any special diagnostics, to enable the flight team to perform anomaly determination and investigation/reconstruction particularly for mission critical activities.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.8.8

2.01.06	**Automated transfer of Data** - Data communication and transfer systems and protocols should be designed to allow for automated transfer of data files/sets between the space and ground segments, space segment elements, and ground segment elements.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-25
2.01.07	**Override Requirement Assessment** - The need for a crew and/or ground initiated override to temporarily or permanently disable an automated function should be addressed for each automated fault detection and critical response function.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-14
2.01.08	**Self Check/Diagnostic Capability** - Automated self-check and self-diagnostic capabilities should be incorporated for ground and space segment systems and components where such capabilities aid in system start-up, operational readiness, time-critical operations, and anomaly assessment.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-17
2.01.09	**Hazardous Command Safeguard** - Flight vehicle and ground-based command systems should be designed to enforce additional safeguards when issuing hazardous commands, including the ability to disable such commands on a temporary basis.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-21
2.01.10	**Automated Fault Detection** - The operational design of space and ground segment systems and components should incorporate automated fault detection, isolation, and recovery (FDIR) where such automation can be demonstrated to improve mission assurance and/or safety.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-12
2.01.11	**Safe Mode Identification** - A safe mode occurrence should be unambiguously identifiable via telemetry.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.3.2
2.01.12	**Bulk data storage** - The information system design should 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 for flight operational uncertainties caused by weather effects or ground tracking station problems.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.8.3

2.01.13	**Sensor reliability for Autonomous Control** - Sensors used to signal a condition to be managed via on-board autonomous control should be reliable, or else inadvertent activation should be shown by analysis to have benign consequences. Sensor reliability should be commensurate with the risk.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.12.1.4
2.01.14	**Avoidance of Inadvertent S/C Off Commands -** In a redundant spacecraft with no hardware failures, no single command should result in Spacecraft "OFF." In a single string Spacecraft, or a redundant Spacecraft with a failure, no single command should result in Spacecraft "OFF."	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.23
2.01.15	**Avoidance of Inadvertent transceiver Off Commands -** Transceiver off commands should be inhibited to avoid inadvertent shutdown of the spacecraft while in flight.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.23
2.01.16	**Control of Command Procedures and Databases** - Command procedures and mission databases (on-board and ground) should be controlled (treated with the same rigor as changes to flight critical software). This includes formal configuration management, peer review by knowledgeable technical personnel, and full verification with up-to-date simulations wherever possible. (Routine loads to perform nominal operations may require less test rigor.)	E.2.05 Product Implementation	GSFC - STD - 1000 Rule 3.14
2.01.17	**End-to-end Data Flow Verification** - The testing of end-to-end data flow, including command and response, should verify that data passes from the originating source to the user destination, without impediment, through flight-like connectivity and processing between ground and space segments.	E.2.07 Product Verification	JSC CxP 72132, paragraph CxP-26

2.01.18	**Flight System/Launch Vehicle Interface Verification** - Early verification of the electrical interfaces between the flight system and launch vehicle should be performed by using an electrical simulator sufficiently in advance of integrated operations to be able to recover from any unexpected incompatibility.	E.2.07 Product Verification	JPL D-17868, paragraph 8.3.8.2
2.01.19	**Command Systems Checks** - Space segment command systems should perform quality/reasonableness checks and parameter bounds on received commands, and results verified on the ground, before they are accepted for execution.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph SS-16
2.01.20	**Command Confirmation** - Every configuration command should have a direct telemetry confirmation.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.38
2.01.21	**S/C Autonomy for Time-Critical Operations -** Space and ground segment systems and procedures should be designed such that mission time-critical operations can be conducted without the need for ground control initiation or intervention.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-11
2.01.22	**Safe Hold Mode** - All spacecraft should have a power-positive control mode (Safe Hold) to be entered in spacecraft emergencies. Safe Hold Mode should have the following characteristics: (1) its safety should not be compromised by the same credible fault that led to Safe Hold activation; (2) it should be as simple as practical, employing the minimum hardware set required to maintain a safe attitude; and (3) it should require minimal ground intervention for safe operation.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.17
2.01.23	**Automated Switchover Notification** - All systems that incorporate an automated switchover capability should be designed so as to provide operator notification of the component malfunction, to confirm that proper switchover has occurred and that the desired system is on line and functioning properly.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-15

3.00	**Contamination Control (CC)**		
3.01	**CC - General**		
3.01.01	**Laser Contamination Control Plan** - All flight laser development should include an approved laser-specific Contamination Control Plan (CCP).	E.2.02 Technical Requirements Definition	GSFC - STD - 1000 Rule 5.08
3.01.02	**Contamination Control Requirements and Processes**- Specific contamination control requirements and processes (such as analytical modeling, laboratory investigations, and contamination protection and avoidance plans) that support mission objectives should be identified early in the project life cycle (at Mission Concept Review) and further developed as the project matures.	E.2.02 Technical Requirements Definition	GSFC - STD - 1000 Rule 4.01
4.00	**Electronic Systems (ES)**		
4.01	**ES - Computer**		
4.01.01	**Computer Reboot** - Computers used during missions for critical operations should be designed for rapid reboot.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-34
4.01.02	**Computing Parameters** - Analyses should be employed early in the lifecycle (By System Requirements Review) to estimate critical computer parameters such as communications bandwidth, throughput, memory (both volatile and nonvolatile), processing speed, and response times. These estimates should be used to define a total capability that allows for margins in the realm of: a.) At computer selection: 75% Margin: b.) At implementation start (start of Phase C/D): 60% Margin: and c.) At launch: 20% Margin where %Margin = 100 * (Total Capability – Estimate) / (Total Capability)	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.1.2.2

4.02	**ES - EEE Parts**		
4.02.01	**EEE Parts Program** - An Electronic, Electrical, and Electromechanical (EEE) parts program should be planned for and implemented for all flight missions for the purpose of part selection, de-rating, screening, and overall qualifications.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 2.02
4.02.02	**Grade-One Parts Vs. COTS** - The availability and cost/risk effectiveness of grade-one parts should be considered before Commercial-Off-The-Shelf (COTS) parts become the design baseline.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.26.1.2
4.02.03	**Parts Derating** - Appropriate derating of parts should be incorporated in electronics design utilizing an approved derating guideline. The guideline requirement is outlined in the Electronic, Electrical, and Electromechanical, (EEE) Parts plan and driven by the Mission Assurance requirements. An example derating guideline would be the GSFC EEE-INST-002, “Instructions for EEE Parts Selection, Screening, Qualification, and Derating.” or possibly some other customer driven derating guideline document. Other examples might be the JSC derating criteria for Space Station environment work, while the JPL guideline would be used for Deep Space Exploration type hardware.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.26.1.1
4.03	**ES - General**		
4.03.01	**Static Bleed Path** - A static bleed resistive path (i.e. 1 M-ohm or greater resistor) should be provided in each assembly from circuit return to the assembly structure.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.2
4.03.02	**Shielding** - High current, high di/dt and dv/dt interface wires should be appropriately shielded/grounded. Furthermore, pyro and power interfaces should be physically separated from signal interfaces as much as practical (e.g., different routing and separate connectors).	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.6

4.03.03	**Back EMF Suppression** - Inductive loads (e.g., valve coils, relays) should be equipped with back-EMF transient suppression.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.7
4.03.04	**Shorts Avoidance** - Power hot, return, and chassis functions should be adequately separated to preclude possibility of hot-to-return or hot-to-chassis shorts. Power connector pin assignments, cable routing, and electronic circuit layouts should receive special attention in designs where the prime power, circuit return, and spacecraft chassis are in close proximity.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.11
4.03.05	**Cable Cut Preparation** - Electrical interfaces passing through cable cutter separation devices should be dead-faced prior to actuation of the device (e.g., signal and power interfaces) should be unpowered.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.12
4.03.06	**Secondary Circuit Design** - Failure in a secondary circuit (telemetry, current monitoring, etc.) should not degrade the primary function.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 2.08
4.03.07	**Current Limiting Architecture Design** - A system current limiting architecture should be developed for all missions, including the payloads.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 2.06
4.03.08	**Transient Effects Avoidance** - Precautions (e.g., time-out) should be taken to prevent adverse effects due to the unpredictable logic states of Field-Programmable Gate Arrays (FPGA's) and Application Specific Integrated Circuits (ASIC's), which can occur at power-on and power-off	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.26.3
4.03.09	**Synchronous Design** - Synchronous design should be used for digital logic to guarantee the sequence of logical decisions and the validity of data transfer.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.27.1

4.03.10	**Synchronous Design Verification** - The synchronous design of Application Specific Integrated Circuits (ASIC) or Field-Programmable Gate Arrays (FPGA) should be verified, as a minimum, by post-route timing analyses using a place and route tool and test vector simulation with timing checkers performed at the primitive level. Timing of boundary conditions (pin-outs) should be constrained both for place, route, and test vector simulation.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.27.2
4.03.11	**Field-Programmable Gate Arrays Model Verification** - Test vectors should be developed and simulations performed to demonstrate the hardware description model design matches behavioral model, the gate level model matches the behavioral model, and fault containment is understood.	E.2.07 Product Verification	LPR 8705, paragraph 3.26.2.3
4.03.12	**Avoidance of Inadvertent Operation** - An electrical disconnect "plug" or set of restrictive commands should be provided to preclude inadvertent operation of components.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.24
4.03.13	**Integrated Circuits Input Isolation** - Integrated circuits, or other devices receiving signals from redundant sides, should incorporate isolation resistors, capacitors, or other elements such that gross failure of the integrated circuit (such as Vcc short to ground) should not compromise both signal sources.	E.2.05 Product Implementation	GSFC - STD - 1000 Rule 2.21
4.03.14	**Power-On Time** - One thousand (1000) hours of operating/power-on time shall be accumulated on all flight electronic hardware (including all redundant hardware) prior to launch, of which at least 200 hours should be in vacuum. The last 350 hours of operating/power-on time should be failure-free.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 2.01
4.03.15	**PCB Testing** - All flight printed circuit boards (PCBs) should be verified by coupon testing.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 2.12

4.03.16	**High Voltage Device Testing** - Assemblies containing a High Voltage supply that are not tested through the Corona region should undergo venting / outgassing analysis to determine when it is safe to turn on and operate after launch.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 2.22
4.03.17	**Solder Joints -** All materials at a solder joint should be selected to avoid the formation of potentially destructive intermetallic compounds for all potential operational environments (temperature, humidity, etc.). Solder joints should be to NASA standards (8739.2, & 8739.3 or the new emerging J-Std-00x with the space addendums). The prohibitive materials requirement should preclude the presence of pure Tin, Zinc and Cadmium on any metal surface including solder. The percentage of Tin in any solder joint or electronic component should be limited to a maximum of 97%.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 4.07
4.03.18	**RDM Level** – Radiation Shielding to a Radiation Design Margin (RDM) of 2 (based on a conservative heritage goal value) is desired at the end of the nominal mission unless the project can demonstrate acceptable risk with a lower margin. Circuit design margins are currently calculated including the combined effects of radiation, temperature, aging, voltage variations, etc. Electrical, temperature, and component derating are major factors to consider when formulating the design margin. Electrical performance and temperature effects may be traded for radiation effects at some risk. A higher chance of degradation at/near the end of the mission may be accepted, provided that mission success is not dependent on at/near end-of-mission events. The component criticality must be taken into account when analyzing the acceptable level of risk. Where spot shielding of a component is to be applied, an RDM of 3 is desired to account for possible unverifiable modeling uncertainties.	E.2.02 Technical Requirements Definition	LPR 8705, paragraph 3.21.2

4.03.19	**EMI Minimization** - Grounding and interfacing should be implemented in the electrical and mechanical design (including packaging) to minimize Electromagnetic Interference (EMI). The grounding and interfacing design should provide the following: An equipotential spacecraft/payload/instrument, and "Faraday" cage where needed; a low conducted and radiated emissions; a high transient noise immunity on circuitry, and prevention or minimization of external and internal electrostatic discharge (ESD).	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.1
4.03.20	**Safe To Mate Verification** - A "safe to mate" verification should be performed after assembly of hardware into the flight system before electrical connections are made and the hardware powered.	E.2.08 Product Validation	JPL D-17868, paragraph 8.3.2.1
4.03.21	**Silicon Junction Temperature Limits -** The thermal design should keep electronic components operating well within their data sheet qualified parameters. For ceramic military temperature range microcircuit components, the operational case temperature limit is 125'C. For other non-standard Electronic, Electrical, and Electromechanical (EEE) parts used temperature rating can be much lower (i.e. commercial 85'C). Additionally, parts should also be thermally derated (typically 15-20%) per NASA derating criteria. Also note that reliability decreases with increasing temperature so mission life requirements may dictate further derating.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.10.2.5
4.03.22	**Parts Failures Analysis** - The root cause of all electronic parts failures should be determined.	E.2.07 Product Verification	LPR 8705, paragraph 3.26.1.3
4.03.23	**Flight Hardware Interface Protection -** Flight hardware interfaces with ground handling and test equipment need to be designed with protective overvoltage/over current or overpressure devices.	E.2.04 Design Solution Definition	LPR 8705.1, paragraph 2.21.1

4.03.24	**Ungrounded Conductive Material** - Space-exposed or “spacecraft-buried” floating conductive materials should be demonstrated to not pose an Electrostatic Discharge (ESD) disruption or damage threat. There should be no ungrounded (floating) conductor >15 cm in length. Grounding techniques are outlined in NASA-HDBK-4001.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.8
4.03.25	**Test Points and Plugs** - All test points and plugs should be capped or protected from discharge for flight.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 2.14
4.03.26	**Circuit Count Margin** - At the start of the Implementation Phase, there should be 30% margin on the spare power switch and circuit count, including cabling and connector pins, to accommodate late identified needs with minimum cost and schedule impact. Circuit count margin should be reported at project Preliminary Design Review (PDR), Critical Design Review (CDR), and start of Assembly, Integration and Test.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.14
4.03.27	**Parts List Review** - An early design parts list review should be performed against documented requirements to: • Identify long-lead time parts. • Assess radiation dose, latch up, and Single Event Effects (SEE) capability/compatibility. • Minimize the number of different part types. • Provide parts vendor assessment information. • Assure all known parts issues are identified and closed early. • Benefit from Parts Engineering/independent assessments and knowledge from other missions • Provide data to project risk database. • Cost-effective match between design and parts capabilities	E.2.03 logical Decomposition	
4.03.28	**Prohibited Materials for Electrical Hardware** - The use of pure tin (tin whiskers), cadmium (out gassing), and zinc plating in flight and ground electrical hardware should be prohibited.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 2.15

4.04	**ES - Interfaces**		
4.04.01	**Non-coaxial Interfaces** - All non-coaxial signal interfaces should use twisted-shielded wire pairs with shields grounded appropriately, unless other wire treatments can be used. Examples of other possible wire treatments are twisted pairs, triplets or no twisting at all depending on applications and the EMI threat.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.4
4.04.02	**External Connectors** - Functions that pass through external connectors (e.g., umbilical, direct access) should be protected in the event of inadvertent connection of any conductor to any other conductor and chassis (i.e. put power on sockets, not on pins, and also use keyed connectors).	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.9
4.04.03	**Use of Common Electrical Interfaces** - The system design should use a common electrical interface approach and circuits to reduce interface designs and protocols.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.24.1
4.04.04	**Minimization of Electronic Interfaces** - The system design should minimize the number and type of interface approaches/circuits used.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.24.2
4.04.05	**Use of Reliable Interfaces** - The system design should consider the use of proven reliable interface types where fault issues, etc. have already been addressed (e.g., 1553 data bus or other avionics standards).	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.24.3
4.04.06	**Flight Connectors Mating** - Mating of all flight connectors which cannot be verified via ground tests, should be clearly labeled and keyed uniquely, and mating of them should be verified visually to prevent incorrect mating.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 2.13
4.05	**ES - Grounding**		
4.05.01	**Circuit Return Path** - Structure or shields should not be used for the primary circuit return path. Wires should be used.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.3

4.05.02	**DC Ground** - Each subsystem ground tree (i.e. power converter secondary) should have a local single point DC ground to chassis via the shortest practical wire length. See also Reference - "A Methodology for Designing Low Noise Systems - Part 2 - Grounding - Revision 1.0"; Date, 10/12, 2010; by Arthur T. Bradley, PhD, PE, NARTE-EMC, Low Noise Systems Laboratory, NASA, LaRC,	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.18.4
4.05.03	**Grounding Concept Design** - A system grounding concept should be developed for all missions. (i.e. grounding map or grounding tree)	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 2.05
4.06	**ES - Power**		
4.06.01	**Critical/ Non-Critical Load Selection** - A critical and non-critical power bus partitioning/loading should be considered. Hardware power bus assignment (critical or non-critical) should be consistent with time critical mission load requirements and maintaining spacecraft safety and ground commandability.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.12.4
4.06.02	**Power Converter Synchronization** - Subsystem power converters should be capable of operating via an externally-supplied synch frequency signal or in a free-running mode near the synch frequency.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.13.2
4.06.03	**Power System Grounding/Fault Tolerance** – The prime power distribution hot and return lines should be DC-isolated from spacecraft chassis such that the maximum fault current is limited to an acceptable level (i.e. a typical 2K-ohm isolation resistor for a 28V system would draw 14mA on a fault to chassis).	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.12.1
4.06.04	**Surge Control/ Load Removal** - Power interfaces should be implemented with in-rush current surge suppression protection and with load removal capability to “clear” a load fault.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.12.3

4.06.05	**Power Margin Through Life Cycle** - Experience indicates there will likely be significant growth to deal with knowns and unknowns in new designs. Adequate margin should be provided to accommodate growth. Based on the system level of the specific LaRC project, system-level power margin shall be at least 30% at the System Requirements Review (SRR), 20% at Preliminary Design Review (PDR), 15% at Critical Design Review (CDR), and 10% at the beginning of assembly, integration and test based on predicted end of life power capability. Significant deviations from the power margin requirements should be accompanied with rationale and recovery options/impacts. Power Margin=Allocation – Current Best Estimate (CBE). % Margin = (margin/allocation) * 100.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.1.2.3
4.07	**ES - Telemetry**		
4.07.01	**Spacecraft State Telemetry** - Onboard telemetry and downlink priorities should be defined to unambiguously report the state of the spacecraft and instruments to ground operators early in each ground tracking pass - specifically identifying any faults experienced.	E.2.09 Product Transition	GSFC - STD - 1000 Rule 3.12
4.07.02	**Real-Time Telemetry During Mission Critical Events** - Mission critical event (Launch Vehicle Separation, deployments) and deployables verification should be available via real-time telemetry.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 7.1.2
4.07.03	**Downlink Data Quality** - The information system and telecommunication system design should meet a default end-to-end downlink data quality average threshold bit-error rate (BER) < 10-6 and an uplink threshold command BER < 10-5 unless otherwise specified by the project.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.7
4.07.04	**Simultaneous Command/telemetry Capability** - The design should permit simultaneous command/telemetry capability using the same antenna or similar coverage antennas.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.10 and 3.10.1.1

4.07.05	**Information System Capability** - The information system design should be capable of passing engineering data through more than one downlink stream.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.9.1
4.07.06	**Early Determination of S/C State -** The telemetry system end-to-end design should permit ground operators, early in the ground tracking pass, to determine rapidly and unambiguously the state of the spacecraft/payload/instrument particularly to determine if the spacecraft/payload/instrument executed a fault protection response.	E.2.08 Product Validation	LPR 8705, paragraph 3.9.7
4.07.07	**Obtaining Spacecraft Up/Down link Frequencies:** Spacecraft typically use communication and telemetry frequencies allocated in a very crowded spectrum bands which are used both nationally and internationally. Therefore processing requests for spacecraft up/downlink frequencies can often take years for approval. Since it is vital not to have your spacecraft operations interfere with other spacecraft operations or vice versa, the government has set up regulations as described in Chapter 10 of the National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedures for Federal Radio Frequency Management to coordinate and provide Radio Frequency Authorization (RFA). NASA provides a Spectrum Manager at each center that will process and coordinate these RFAs. Once the RFAs are completed the Spectrum Manager will send them to NTIA for final approval. Since this is a long process it is essential to get with your spectrum manager as early as possible. (Continued below.)	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.9.5

4.07.07 Cont.	You are ready to do this when you have Authority to Proceed with the project and you have all of the RF data package ready. (This is the data the spectrum manager needs for processing – the spectrum manger will provide a work sheet to be filled out) This should be coordinated between the project spacecraft and ground system managers and the spectrum manager. The spectrum manager can also process orbital slot allocations. The project should have the spectrum manager process this along with the RFAs.		
4.07.08	**Measurement Predictions and Alarm Limits** - Subsystem telemetry measurement predictions and alarm limits should be developed and in-place prior to planned spacecraft/payload/instrument operations to provide rapid assessment of operational performance and provide an early alert of potential spacecraft/payload/instrument problems.	E.2.04 Design Solution Definition	LPR 8705, paragraph 4.7
4.07.09	**On-board Recording Capacity -** The capabilities for on-board recording of telemetry data and downlink of the recorded data should be designed with consideration for both nominal and contingency operational scenarios. Telemetry recording should accommodate margin in the form of higher sampling rates and additional partners.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph SS-18
4.07.10	**Link Margins at PDR -** At implementation start, nominal link margins should be at least 6 dB. Links with extreme geometry conditions, surface-to-orbit links, or surface-to-surface links should consider 10 dB or more margin depending on the nature, complexity, and scope of design uncertainties.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.9.6

5.00	**Guidance Navigation and Control (GN&C)**		
5.01	**GN&C General**		
5.01.01	**Flight Control System Stability Margins -** For design purposes, linear analysis is typically used to develop systems with adequate robustness. For control system design, industry standards of at least 6 db gain margin and at least 30 degrees of phase margin should be specified for design conditions for rigid-body stability. If flexible modes are gain stabilized, gain margins for those modes should be increased to at least 12 db (20 db gain margin typical). For modes using phase stabilization, phase margins of 45 degrees (front side – lower frequencies) and 60 degrees or more (back side – higher frequencies) should be used. The increased backside phase margin is important because lags and delays that might not be properly accounted for in the modeling of actuators and overall system tend to reduce the higher frequency phase margin. Note: - There are often times where a mode might be unstable during a small part of the flight envelope of the vehicle – particularly for a launch vehicle that is experiencing rapidly changing vehicle and flight conditions. Even though linear analysis may show an instability, if the time to double is long compared to the amount of time the vehicle is in that condition, that might also be acceptable. (Continued below.)	E.2.04 Design Solution Definition	LaRC - Jay Brandon

5.01.01 Contd.	The stability characteristics of the flight control system should be analyzed with a high fidelity nonlinear simulation including important effects such as aerodynamics, mass properties, actuator system dynamics, structural dynamics, slosh, etc. Variations of the models of the systems should be made to determine the sensitivities the system exhibits due to off-design conditions that might occur due to modeling errors. The nonlinear, high fidelity analyses should be considered the “best” prediction of system performance. The combined approach of linearized analyses along with high-fidelity nonlinear simulation analysis provides a good approach of assessing the impact of a locally unstable mode indicated in linear analysis, and this assessment should be done before sacrificing vehicle rigid-body stability, other modal stability, or performance by attempting to provide global coverage of the gain and phase margin requirements.		
5.01.02	**Flight Control System Actuator Sizing** - The Flight Control System (FCS) actuator sizing should reflect specified allowances for mass properties growth.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.31
5.01.03	**Stray-light Input Analysis -** Stray-light input should be considered and effects precluded /minimized particularly for attitude control celestial reference sensors and science imaging instruments (e.g., visible, IR, and UV spectral regions).	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.23.2
5.01.05	**Fault Protection Testing** - When redundancy has been used in the flight system design to provide fault tolerance, system fault protection testing should verify the timeliness of switching between redundant elements, in addition to verifying the availability of the redundant functionality.	E.2.07 Product Verification	JPL D-17868, paragraph 8.3.5.1

5.01.06	**GN&C Device Testing** - All GN&C sensors and actuators should undergo end-to-end phasing/polarity testing after spacecraft integration and should have flight software mitigations to correct errors efficiently.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 1.07
6.00	**Mechanical Systems (MS)**		
6.01	**MS - Mass**		
6.01.01	**Mass Margin Allocation Vs. Time -**In order to define the nomenclature necessary to discuss Mass Margin refer to Figure 6.01.01 below with the following definitions. **Current Best Estimate (Basic Mass in AIAA S-120-206) :** The current mass data based on an assessment of the most recent baseline design. The design assessment includes the estimated, calculated, or measured, (or actual) mass, and includes an estimate for undefined design details like cables, multilayer insulation and adhesives. **Mass Growth Allowance (MGA)**: Predicted change to the basic mass of an item based on an assessment of the design maturity and fabrication status of the item (See Table 6.1.1a, below, adapted from AIAA Standard S-120-2006 (Mass Properties Control for Space Systems)). Technology Readiness Level (TRL) assignment can also be used in design maturity assessment (See Table 6.1.1b, below, from GSFC Gold Rules). **Predicted Mass (Dry)**: Basic Mass plus the Mass Growth Allowance. **Allowable Mass (Dry)**: Allowable Mass minus Maximum Propellant Mass. Note: There is no mass margin in the propellant mass. The propellant margin is carried in the Delta-V (Continued below.)	E.2.04 Design Solution Definition	LaRC Engineering Staff, AIAA S-120-2006 and GSFC - STD - 1000

6.01.01 Cont.	**Allowable Mass:** Allocated mass to the system/subsystem derived from the requirements decomposition. **Mass Margin:** Allowable Mass (Dry) Minus Predicted Mass (Dry). **Reserve:** Optional mass budget reserved by the customer for out-of-scope changes. Reserve is held at the next higher level. Program holds the project reserve. The system holds the subsystem reserve. If reserve is not held then Mass limit = Allowable Mass **Mass Limit:** Absolute Mass limit - Typically based on launch-vehicle-to-orbit performance capability **%Mass Margin** = ((Allowable Mass Dry - Predicted Mass Dry) Over Predicted Mass Dry) X 100 When developing a space system the standard rule-of thumb to be applied to the sum of the MGA and the Margin is as follows. At SRR (MGA + Margin) Greater than or equal to 30% At PDR (MGA + Margin) Greater than or equal to 20% At CDR (MGA + Margin) Greater than or equal to 10%		

Figure 6.01.01

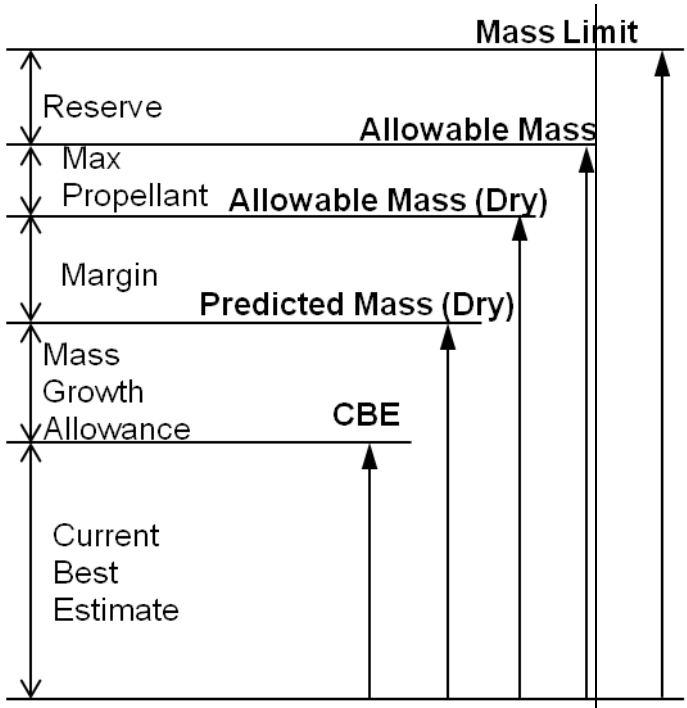


Table 6.01.01a

Table 1 — Mass Growth Allowance and Depletion Schedule

Major Category	Maturity Code	Design Maturity (Basis for Mass Determination)	Mass Growth Allowance (%)												
			Electrical/Electronic Components			Structure	Brackets, Clips, Hardware	Battery	Solar Array	Thermal Control	Mechanisms	Propulsion	Wire Harness	Instrumentation	ECLSS, Crew Systems
			0-5 kg	5-15 kg	>15 kg										
E	1	**Estimated** 1) an approximation based on rough sketches, parametric analysis, or undefined requirements, 2) a guess based on experience, 3) a value with unknown basis or pedigree.	30	25	20	25	30	25	30	25	25	25	55	55	23
	2	**Layout** 1) a calculation or approximation based on conceptual designs (equivalent to layout drawings), 2) major modifications to existing hardware	25	20	15	15	20	15	20	20	15	15	30	30	15
C	3	**Preliminary Design** 1) calculations based on a new design after initial sizing but prior to final structural or thermal analysis, 2) minor modification of existing hardware	20	15	10	10	15	10	10	15	10	10	25	25	10
	4	**Released Design** 1) calculations based on a design after final signoff and release for procurement or production, 2) very minor modification of existing hardware, 3) catalog value	10	5	5	5	6	5	5	5	5	5	10	10	6
A	5	**Existing Hardware** 1) actual mass from another program, assuming that hardware will satisfy the requirements of the current program with no changes, 2) values based on measured masses of qualification hardware	3	3	3	3	3	3	3	2	3	3	5	5	4
	6	**Actual Mass** measured hardware	No mass growth allowance – use appropriate measurement uncertainty values												
	7	**Customer Furnished Equipment or Specification Value**	Typically a "not-to-exceed" value is provided; however, contractor has the option to include MGA if justified												

Table 6.01.01b

Table 1.06-2 Recommended Mass Contingency/Reserve by Subsystem[1]

All values are assumed to be at the end of the phase

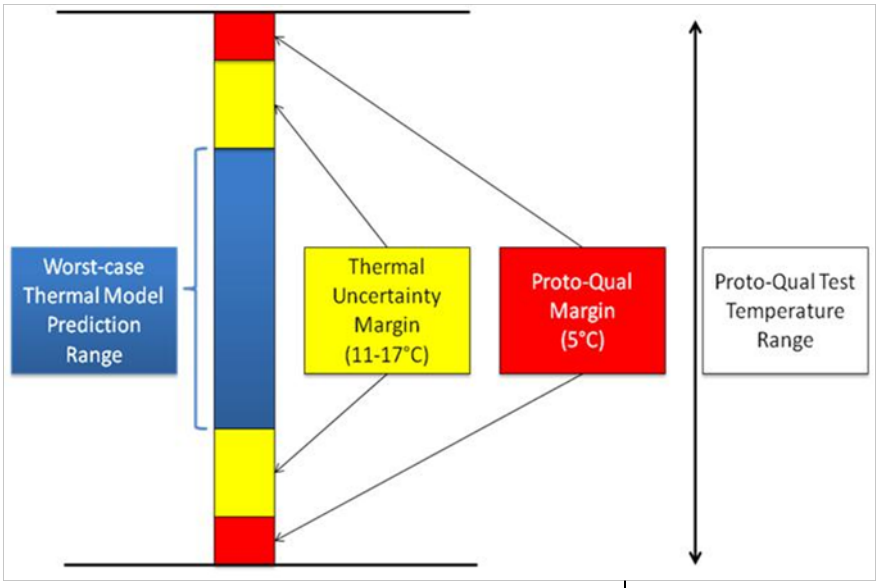
Sub-system Design Maturity[2]	TRL Range[2]	Contingency/Reserve (in percent)[3]											
		Electrical/Electronic											
		0-5 kg	*5-15 kg*	*>15 kg*	*Structure*	*Brackets, Clips, Hardware*	*Battery*	*Solar Array*	*Thermal Control*	*Mechanisms*	*Propulsion[4]*	*Wire Harness*	*Science Instrument*
Basic principles reported thru technology concept and/or application formulated.	0 to 2	30	25	20	25	30	25	30	25	25	25	55	55
Analytical/experimental proof of concept thru breadboard validation in relevant environment	3 to 5	25	20	15	15	20	15	20	20	15	15	30	30
Sub-system/component prototype demo in an operational environment	6	20	15	10	10	15	10	10	15	10	10	25	25
Sub-system engineering unit test in an operational environment	7	10	5	5	5	6	5	5	5	5	5	10	10
Actual sub-system completed and flight qualified	8	3	3	3	3	3	3	3	3	3	3	5	5
Actual sub-system flight proven through successful mission operations	9	0	0	0	0	0	0	0	0	0	0	0	0

1. Adapted from Table 1, "Space Systems - Mass Properties Control for Space Systems",S-120-2006e, AIAA.
2. See the latest version of NPR 7120.8 Appendix J for NASA TRL definitions and classification schema.
3. Contingency % =100% x Contingency(kgs)/(Maximum Expected Value(kgs) - Contingency(kgs))
4. Propulsion sub-system dry mass only.
5. For system margins, see Table 1.06-1.
6. Subsystems not identified as new technology developments can be evaluated as if they are at TRL 6.
7. Subsystems which are fully qualified at the system level for the current mission, and have been weighed, can be evaluated as if they are at TRL 9

6.01.02	**Mass Allocation Methodology** - When defining mass allocations and margins consider that the Power and Propulsion systems should be sized to their maximum requirements before allocating the rest of the Mass Growth Allowances and the Margin. Also the Allowable Mass should be used by the spacecraft structural subsystem to size the core spacecraft structure.	E.2.04 Design Solution Definition	
6.01.03	**Mass/Propellant Margins** - For systems at the spacecraft level, mass needs to account for on-board propellants. The propellant load needs to be sized to provide the required delta velocity for the allowable mass. Note: Propellant margin is based on delta Velocity margin.	E.2.14 Technical Configuration Management	LPR 8705, paragraph 3.1.1.7

6.01.04	**Mass Properties Variability** - The systems effects of propellant-slosh dynamics and other sources of variability in spacecraft or payload system-level mass properties should be accounted for when applicable. In particular, the effects on stability, pointing accuracy, and fault protection should be addressed. Methods of positive mass property control (e.g., propulsion latch valves, trim orifices) should be incorporated into the design to preclude unacceptable fluid migration or mass property change.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.6
6.02	**MS - Structures**		
6.02.01	**Mechanical Clearance Analysis** - Analysis of mechanical clearances during the design phase should be performed using linear addition of tolerances in the worse case environments (i.e. temperature limits). Verification of the clearances in the as-built hardware should again consider worse case environments.	E.2.07 Product Verification	LPR 8705, paragraph 2.23.8
6.02.02	**Integrated Design Interactions** - The integrated design of structure, deployed appendages, and the attitude control response should preclude/minimize possible interactions caused by lower order modal frequencies.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.19.5
6.02.03	**Use of Positive Location System** - When precise location of a component is required, the design should use a stable, positive location system (not relying on friction) as the primary means of adjustment.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 4.22
6.02.04	**Static load Testing** - Static load testing should be required for all primary structures as a part of qualification and to demonstrate margin.	E.2.07 Product Verification	LPR 8705, paragraph 3.26.1.4
6.02.05	**Avoidance of Sensor & Antenna Blockage** - When a spacecraft is in its stowed (launch) or deployed configuration, it should not obscure visibility of any attitude sensors required for acquisition, and it should not block any antennas required for command and telemetry.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.37

6.02.06	**Field of View Clearance** - The configuration design should provide an appropriate amount of additional clearance beyond nominal specified Fields of View (FOV's) to preclude/minimize obscuration effects (e.g. to sensors, antennas, and thrusters) caused by structural elements, blankets, booms, covers, etc.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.23.1
6.03	**MS - Thermal**		
6.03.01	**Thermal Test Limits** - Components and systems should be tested beyond allowable flight temperature limits. For component level tests, the margin for protoflight thermal vacuum testing should be 5°C beyond thermal model predictions, after thermal model uncertainty has been applied, as shown in Figure 6.03.01, below. Thermal uncertainty will be based on state of model correlation at the time of the test; in general, thermal uncertainty for uncorrelated models should be 17°C, and for correlated models can be reduced to 11°C. For active control systems with a fixed set point, margin should be demonstrated by increasing or decreasing (as appropriate) the heat load (internal or external) by at least 30% and still maintaining the control temperature. (Continued below.)	E.2.07 Product Verification	GSFC - STD - 1000 Rule 4.27 and LaRC input
6.03.01 Cont.	For cryogenic systems, this thermal uncertainty margin of 11°C will generally represent an excessively large fraction of the operating range; a smaller margin on a program-specific basis, based on those given in Spacecraft Thermal Control Handbook, Chapter 15 & 19, can be used. Component level tests of electronics and spacecraft mechanisms should be qualified by thermal vacuum testing over at least a 55°C total range (at the mounting or thermal control surface for the specified assembly), or flight temperature limits extended by +/- 10°C , whichever is greater. For system level tests, in general the worst case component in each thermal zone will be used to set target temperatures.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 4.27 and LaRC input

Figure 6.03.01			
6.03.02	**Thermal Balance Test** - All subsystems/systems having a thermal design should be subject to a Thermal Balance Test at the appropriate assembly level. The intent of this test is to verify and validate the thermal model of the system.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 4.28
6.03.03	**Thermal Vacuum Testing for Systems and Components in Unpressurized Areas** - All systems flying in unpressurized areas should have been subjected to a minimum of eight (8) thermal-vacuum test cycles prior to launch. Four (4) of these cycles may include cycles at the subsystem or instrument level of assembly. This number may also include cycles done at a spacecraft level. Flight hardware thermal cycling should be minimized to preclude the risk of damage. If a component has never flown, a larger number of component level cycles should be done, with the exact number decided on a case-by-case basis.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 4.29

6.03.04	**Thermal Control for Propellant Interaction** - Hardware that will come in contact with propellant or propellant vapor should be thermally controlled during any period when propulsion system may be active to remain safely (>10° C) above the temperature at which propellant condensation will occur.	E.2.02 Technical Requirements Definition	LPR 8705, paragraph 3.11.8
6.03.05	**Thermal Design Margin** - The thermal design margin needs to be non-negative for all mission-enabling and mission-critical modes of operation. Thermal design margin is the difference between the flight-allowable temperature range and the worst-case hot and cold predicted temperatures. Worst case is that combination of realistic thermal extreme environments and loads that produces the maximum hot and minimum cold predicted temperatures. Consideration should be given to performing probabilistic analysis to provide the worst case, rather than stacking many parameters simultaneously at their worst case extremes. Thermal design should be tailored to the specific applications of the mission with consideration for both equipment reliability and temperature/performance interactions. The thermal design should maintain temperatures within flight limits with a +/-10°C margin. Components that are actively controlled may have a reduced margin of +/- 5°C, and may use a heater power margin of 25% on the cold side, in lieu of the temperature margin. (Continued below.)	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.10.2.4

6.03.05 Cont.	Note: This applies to normal operations and planned contingency modes. This does not apply to cryogenic systems or entry/TPS systems. Cryogenic systems may use the guidelines given in the Spacecraft Thermal Control Handbook, Chapter 15 & 19, which vary the recommended margin for cryogenic systems based on the temperature range of interest of the system. Entry/TPS systems may utilize a project-specific required thermal margin, since in general both temperature ranges and thermal extremes are higher. Thermal design margins must be planned in concert with other margins already applied, such as margins on aeroheating loads and TPS thickness.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.10.2.5
6.03.06	**Thermal Coatings Properties for Analysis** - All thermal analysis should employ thermal coatings properties that are determined to be accurate for materials and mission flight parameters over the lifecycle of the mission.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 4.06
7.00	**Operations (OP)**		
7.01	**OP - Design**		
7.01.01	**Minimization of Uplink and Downlink Transfers** - Space and ground segment command and data handling systems should be designed to minimize the size and frequency of uplink and downlink transfers for executing nominal operations. Also see C&DH - General - 2.01.01.	E.2.04 Design Solution Definition	JSC CxP 72132, paragraph CxP-22
7.01.02	**Flight Systems and Flight Operations Concurrent Design** - The flight systems and flight operations design should be developed concurrently to enable cost-effective end-to-end operations.	E.2.04 Design Solution Definition	LPR 8705, paragraph 4.1.1
7.01.03	**Operational Complexity Minimization** - The flight systems should consider methods to reduce operational complexity and interdependencies (e.g. require less calibration, provide more on-board closed-loop control, provide robust technical margins, provide more autonomy).	E.2.04 Design Solution Definition	LPR 8705, paragraph 4.1.2

7.02	**OP - Test**		
7.02.01	**Mission Preparation Tests** - Mission preparation tests should require a minimum of 1 successful end-to-end tests (to include launch and early orbit simulations), and 1 day-in-the-life simulations with the flight ops team running the flight system. Flight operators should participate as test conductors during integration and test (I&T) at a minimum as specified in the tests above.	E.2.08 Product Validation	GSFC - STD - 1000 Rule 3.10
7.02.02	**Ground Based Testing During Flight Operations -** Projects should maintain the ability to do functional and performance testing related to in-flight operational issues (software changes, constraints, parameter updates, etc.) for the lifetime of the mission. This includes maintenance of avionics flight-like equipment, commercial equipment and software emulators in the ground test environment. A plan for maintaining this capability, which addresses hardware aging and obsolescence, should be included as part of the overall operations plan and reviewed regularly over the life of the mission.	E.2.08 Product Validation	JSC CxP 72132, paragraph CxP-38
7.02.03	**Validation Through Operational Readiness Testing** - Demonstrate, through operational readiness testing, that the people and procedures function effectively in flight-like operations environments including all voice, command, telemetry and decision paths, as well as in a realistic mission timeline.	E.2.08 Product Validation	NPR 8705, paragraph 2.22.3
7.03	**OP - Rules**		
7.03.01	**Flight Sequence Testing** - All flight sequences should have been tested on a high fidelity flight-like system test bed and all anomalies dispositioned prior to commanding.	E.2.07 Product Verification	LPR 8705, paragraph 4.2.2

7.03.02	**Launch and Mission Critical Sequences** - The launch sequence and other mission critical sequences should be test-verified on the spacecraft/payload/instrument before launch under nominal and faulted conditions using the final load flight software. If resources or other factors do not permit testing of critical mission sequences, the system test bed may be used for verification.	E.2.07 Product Verification	LPR 8705, paragraph 4.2.6
7.03.03	**Early Demonstration of Functional Capabilities** - The flight operations team should consider early demonstration of spacecraft/payload/instrument functional capabilities prior to actual mission need to characterize and evaluate the spacecraft/payload/instrument and ground system end-to-end operation. Early characterization/evaluation enables the project to identify flight/ground system shortfalls and make changes safely and reliably with minimal threat to the mission.	E.2.02 Technical Requirements Definition	LPR 8705, paragraph 4.10
7.03.04	**Mission Time-Critical Operations -** After initiation, mission time-critical operations should *not* require "ground-in-the-loop" commanding to enable successful operation/completion. Also see C&DH - General - 2.01.21.	E.2.04 Design Solution Definition	LPR 8705, paragraph 4.2.4 and 4.2.5
7.03.05	**Critical Event Contingency Plans** - For at least mission critical and first time in-flight events, contingency plans should be developed to minimize the threat to health/safety of the mission in case of unexpected/improper spacecraft/payload/instrument response.	E.2.09 Product Transition	LPR 8705, paragraph 4.5.1
7.03.06	**Launch Sequence Design**- Completion of the launch sequence should leave the spacecraft/payload/instrument in a ground-commandable, safe state requiring no "immediate" time-critical ground commanding to assure health/safety.	E.2.09 Product Transition	LPR 8705, paragraph 4.2.7
7.03.07	**System Developers Involvement in Operations** - System developers need to be involved in conducting flight operations particularly in the early operations activities following launch.	E.2.09 Product Transition	LPR 8705, paragraph 2.21.3

7.03.08	**Transmitter-Off Command Inhibit** - Transmitter-Off Command must be inhibited prior to flight. After in-flight turn on, the spacecraft downlink RF transmitter hardware should not be turned off during nominal flight operations. The transmitter should remain powered during the entire mission unless momentarily power cycled via system autonomous fault protection responses. The inhibit may be in the flight or ground system, (i.e. Ground system to inhibit the "off command" upload.) Also see C&DH - General - 2.01.15.	E.2.09 Product Transition	JPL D-17868, paragraph 9.3.1
7.03.09	**Mission-Critical Event Telemetry Coverage** -Continuous telemetry coverage should be maintained during all mission-critical events. Mission-critical events should be defined to include separation from the launch vehicle; power-up of major components or subsystems; deployment of mechanisms and/or mission-critical appendages; and all planned propulsive maneuvers required to establish mission orbit and/or achieve safe attitude. After separation from the launch vehicle, continuous command coverage should be maintained during all following mission-critical events.	E.2.09 Product Transition	GSFC - STD - 1000 Rule 1.14
7.03.10	**Flight Rules Constraints on Flight Sequences -** Flight sequences should operate the spacecraft/payload/instrument consistent with flight rules provided by the developers and within environments and functional regimes experienced during development testing. Any planned operation beyond that ground tested should be tested prior to flight use to demonstrate safe, reliable functionality, and acceptable margin.	E.2.09 Product Transition	LPR 8705, paragraph 4.2.1
7.03.11	**Avoidance of Power Cycling** - Power cycling of mission-critical hardware should be avoided.	E.2.09 Product Transition	LPR 8705, paragraph 4.11.1

7.03.12	**Flight S/W Loads Verification** - Flight software loads/updates, and sequence memory loads, particularly for those affecting mission critical capability, should be verified by a memory readout or checksum readout. Depending on the application and mission/system consequence, single or multiple readouts shall be considered.	E.2.09 Product Transition	LPR 8705, paragraph 4.2.9
7.04	**OP - Training**		
7.04.01	**Train As You Fly** - Train as you will fly, fly as you trained. Make training scenarios as close as possible to foreseen situations.	E.2.09 Product Transition	JSC CxP 72132, paragraph MOS-15
7.04.02	**Capture Knowledge From Training** - Establish a formal process to capture all simulation and training knowledge and lessons learned.	E.2.09 Product Transition	JSC CxP 72132, paragraph FE-16
8.00	**Reliability (Rel)**		
8.01	**Rel - Fault and Failure Protection**		
8.01.01	**Fault Protection During Critical Mission Activities** - During critical mission activities (e.g., launch, orbit insertion), the flight fault protection response should autonomously re-establish the needed spacecraft functionality to permit safe, reliable, and timely completion of the mission critical activity.	E.2.04 Design Solution Definition	LPR 8705 paragraph 3.5.2
8.01.02	**Fault Protection for Non-Critical Periods** - Following a fault condition during non mission-critical orbiting or cruise periods, the flight protection response should at a minimum, autonomously configure the spacecraft to a safe, quiescent, ground-commandable state.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.5.1
8.01.03	**Fault Protection Commandability** - The fault protection system design should be in-flight commandable to permit changing the state of enable/disable parameter and other pertinent parameters (e.g., threshold and persistence values). The status of these parameters shall be telemetered and made available for timely flight team use.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.3.3LPR 8705, paragraph 3.4

8.01.04	**Fault Protection Sensitivity** - Spacecraft/Payload/Instrument Autonomous fault protection enable/ disable strategy, threshold trigger values, and persistence values should be established considering mission phase applicability and operational activity. The enable/disable, trigger, and persistence values should be selected to ensure safety but not “hair triggered” to cause inadvertent F/P entry/execution	E.2.04 Design Solution Definition	LPR 8705, paragraph 4.9
8.01.05	**Co-Located Element Failure Effects Avoidance** - Failure in a physically co-located redundant element should not cause damage to, or interfere with the proper operation of, other redundant elements (explosive decomposition, emission of contaminants).	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.18
8.01.06	**Fault Tolerance for Space Systems -** If a system failure may lead to a Catastrophic Hazard, the system should have three independent, verifiable inhibits (dual fault tolerant). If a system failure may lead to a Critical Hazard, the system should have two independent, verifiable, inhibits (single fault tolerant). Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" (DFMR) areas of design, and have separate, detailed safety requirements that they must meet. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.26

8.01.07	**Non-Essential Circuitry Faults** - The design should ensure that faults in non-essential circuitry do not propagate to essential functional elements (failure of a telemetry monitor circuit should not propagate to the functional element whose performance is being monitored). This should be shown through the process of conducting an assembly/component level Failure Mode Effects Analysis (FMEA). The results from this analysis would be used for generating the critical item list for the project and identifying the direct and indirect effects between the essential and non-essential circuitry.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.12.1.6
8.01.08	**Avoidance of Loss of Mission Due to Single Failure -** It is a major design goal to have no credible single failure of any electrical, mechanical, optical, electro-optical or electromechanical element result in the loss of the entire mission.	E.2.04 Design Solution Definition	LPR 8705.1, paragraph 2.7.1
8.01.09	**Single-point Failure Risk Management -** Single point failures that inhibit the ability to fully meet minimum mission success requirements should be identified, and the risk associated with each should be characterized, managed, and tracked. A Single Point Failures list should be developed, maintained and addressed at System Requirements Review (SRR), Preliminary design review (PDR), Critical Design Review (CDR), System Acceptance Review (SAR), and Flight readiness Review (FRR).	E.2.04 Design Solution Definition	LPR 8705.1, paragraph 2.7.4
8.02	**Rel - Redundancy**		
8.02.01	**Redundant Systems Independence** - When redundant systems or functions are implemented for risk mitigation, the redundant components, or functional command paths, should be electrically, thermally, mechanically and functionally independent, such that the failure of one component or command path does not affect the other component or command path.	E.2.04 Design Solution Definition	GSFC - STD - 1000 Rule 1.25

8.02.02	**Single-point Failures in Redundant Processing Strings** - Redundant processing strings, such as command and data handling, should be designed to avoid single-point failures that incapacitate all strings (an element such as shared memory that is susceptible to corruption of hardware failure.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.14
9.00	**Software (SW)**		
9.01	**SW - General**		
9.01.01	**S/W Design for Test** - The software design should enable testing at all levels, including self-test and built-in routines, that facilitate incremental test operations and fault diagnostics. The test features should be either easily removable or have safeguards to ensure they cannot inadvertently cause damage or interfere with operations during flight.	E.2.04 Design Solution Definition	LPR 8705.1, paragraph 2.18.2
9.01.02	**S/W Support of Computer Resources Measurements** - The flight software should be designed to support measurement of computing resources such as throughput and memory. All margin and performance estimates are considered speculative until measured. External instrumentation is recommended.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.2.2
9.01.03	**S/W Support of Fault Protection** - Fault case issues should be addressed and solutions incorporated into the design during the design cycle. Fault protection software should be specified in the systems engineering process to handle all credible flight system single -fault scenarios.	E.2.04 Design Solution Definition	LPR 8705, paragraph 2.31.6
9.01.04	**Software Logic Design** - Software logic design and its implementation in code should be based on the following: a.) Diagrams that depict flow of control, state transitions or equivalent graphics that facilitate comprehensive evaluation of the execution paths; b.) An analysis of possible software failures and c.) Explicit consideration of off-nominal behavior and possible failure of interfacing hardware	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.1.2

9.01.05	**S/W Input/Output Data Design** - Software should be specified and designed to tolerate and continue functioning when failed input/output transactions or other interactions are temporarily missing or fail to complete. Data should be specified by attributes such as type, nominal values, precision, allowable ranges, originator (source), and dependencies.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.3.3
9.01.06	**Detection of Data Faults** - Flight software should be designed to detect and respond to incorrectly formatted commands, data, loads and memory faults allocated to the software, such as stuck bits or Single Event Upsets (SEU). Software designs need to include check sum logic and periodic verification of memory to detect command, data, load, and memory faults.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.2
9.01.07	**S/W Modification Protection** - Flight software that is intended to be modifiable during flight should be protected from unintended modifications (e.g. input commands should be verified).	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.3
9.01.08	**S/W Resource Over-usage Accommodation** - Software design should accommodate unintended situations where resource usage is oversubscribed. The action to be taken in such situations should be specified as part of the requirements on the design.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.5
9.01.09	**S/W Processing Failure Accommodation** - Software should be designed to detect failures to complete an intended processing path or loop, and restore the processing.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.7
9.01.10	**S/W Memory Protection** - Software should be designed for memory integrity by protecting against buffer overflows and pointer manipulations while managing the executable and data memory regions.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.11
9.01.11	**S/W Interrupt Tolerance** - Software should be designed to ensure that data sets and parameter lists are consistent with respect to time when passed among processes such as software subsystems, rate groups and others. For example, software should not be interrupted in a	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.12

	manner that permits it to use both old and new components of a vector.		
9.01.12	**S/W Deadlock Avoidance** - Software should be demonstrated to be free of deadlocks. A deadlock is the condition where two processes cannot proceed because they both simultaneously require the exclusive use of shared resources held by one another.	E.2.04 Design Solution Definition	JPL D-17868, paragraph 4.11.4.13
9.01.13	**Code/Software Updating** - The updating of code/software should be limited to a single target memory device under user ground control and monitoring. Under no circumstances should prime and redundant memories be modified concurrently, or before the operational performance of the change is properly assured in a single unit.	E.2.05 Product Implementation	GSFC - STD - 1000 Rule 3.13
9.01.14	**Dead S/W Code Avoidance** - Dead software (SW) code (unused or unreachable code) is undesirable and should be avoided. Dead software code should be analyzed by the software development and system safety teams to ensure safety hazards and mission risks are addressed that could be caused by the software's removal or if not removed, by the abnormal conditions that could arise from unintended execution.	E.2.05 Product Implementation	GSFC - STD - 1000 Rule 3.02
9.01.15	**FSW Long Duration Testing** - Ground test of the fully integrated Flight Software (FSW) system should include an uninterrupted long duration test performed at the system level that includes demonstration of error free operations-like scenarios over an extended time that could be masked by routinely restarting the system, as is typical in a test program. Long-duration testing is beneficial for detecting "memory leaks" that might lead to degraded or unpredictable performance after a long run time.	E.2.08 Product Validation	GSFC - STD - 1000 Rule 3.11

9.01.16	**FSW Regression Testing** - New versions of flight software should undergo regression testing on the flight vehicle prior to use in system level verification. Regression testing demonstrates that there are no obvious, unintended changes to the software and verifies the capabilities.	E.2.07 Product Verification	JPL D-17868, paragraph 8.3.2.2
10.00	**System - (Sys)**		
10.01	**Sys - General**		
10.01.01	**Use of Lessons Learned** - The design should be reviewed early in the formulation process and at appropriate points in the life-cycle by the engineering team against the LaRC/NASA Lessons Learned data base, NASA Alerts, etc. Items of potential applicability to the project should be identified and dispositioned.	E.2.04 Design Solution Definition	LPR 8705.1, paragraph 2.14
10.01.02	**Design Robustness Considerations** - The design robustness should include consideration of the following: Inadvertent operation outside expected flight environments, e.g., temperatures, radiation dose; shortfalls in performance, e.g., RF power output, antenna gain; fault propagation due to collocation of components, e.g., thrusters, adjacent redundant electronic components on the same chip.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.22
10.01.03	**System Design Verification Plan** - The design verification plan needs to provide for early system functional and performance verifications. In particular, system level verifications need to include testing of appropriate flight sequences under both nominal and simulated faulted conditions, verifications of interfaces with the spacecraft/Launch Vehicle, the Ground Data System, and other project unique interfaces. The plan needs to require a system level electrical “plugs-out” test using the minimum number of test equipment connections.	E.2.07 Product Verification	LPR 8705.1, paragraph 2.23.5

10.01.04	**Spare Units Plan** - All projects should define a plan for required spare units (including spare Electronic, Electrical, and Electromechanical (EEE) parts) that is compatible with available resources and acceptable risk.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 1.10
10.01.05	**Polarity, Orientation, Position Verification** - All hardware should be verified by test or inspection of the proper polarity, orientation, and position of all components (sensors, switches, and mechanisms) for which these parameters affects performance.	E.2.07 Product Verification	GSFC - STD - 1000 Rule 1.33
10.01.06	**Statistical Analysis Approach Definition** - The approach (e.g., linear sum, root-sum-square, confidence level) for combining system performance contributors' nominal values plus uncertainties should be defined for each performance measure. The statistical combining approach should take into account the dependence/coupling of the contributors, the nature of the uncertainties (systematic or random), and the uncertainty distributions (Gaussian, uniform, etc.).	E.2.04 Design Solution Definition	LPR 8705.1, paragraph 2.13.1
10.01.07	**Thruster Plume, Venting Analysis** - Thruster or external venting plume impingements should be precluded/minimized.	E.2.04 Design Solution Definition	LPR 8705, paragraph 3.23.3