Langley Research Center

Directive: LPR 8705.1

Effective Date: July 22, 2004

Expiration Date: June 4, 2008

Design, Verification/Validation, and Operations Principles for Space Flight Systems

National Aeronautics and Space Administration

Primary Office of Responsibility: Systems Engineering Competency

PREFACE

P.1 PURPOSE

This document addresses the principles to be followed/utilized in the formulation and implementation phases for LaRC space flight projects. These principles cover hardware and software design/development, margins, design verification, flight operations control and monitoring, and the integration of safety and mission assurance into these areas.

P.2 APPLICABILITY

These principles apply to all space flight systems including, but not limited to, major instruments, payloads, and/or spacecraft. They apply to the system contractor/partner as well as in-house/sub-system project implementation functions.

P.3 AUTHORITY

a. NPD 7120.4, “Program/Project Management.”
b. NPD 2820.1, “NASA Software Policies.”
c. NPD 8730.4, “Software Independent Verification and Validation (IV&V) Policy”

P.4 REFERENCES

a. NPR 7120.5, “NASA Program and Project Management Processes and Requirements.”
b. LPR 5300.1, “Space Product Assurance.”
c. LPR 7122.1, “Systems Engineering Handbook for In-House Space Flight Projects.”
d. LMS-CP-1360, “Planning, Definition, and Development of Instruments within Atmospheric Sciences.”
e. LMS-CP-1380, “Science Satellite Mission Operations.”
f. LMS-CP-5502, “Systems Engineering Requirements Definition and Implementation Planning for Research Projects/Experiments.”
g. LMS-CP-5505, “Flight Project and Experiments Review Planning and Implementation in Accordance in NPR 7120.5.”
h. LMS-CP-5506, “Aerospace Systems Implementation, Testing, and Integration within Systems Engineering.”
i. LMS-CP-5507, “Reporting and Disposition of Nonconforming Aerospace Hardware Items and Products.”
j. LMS-CP-5508, “Ad Hoc Technical Review (including Tiger Teams).”
k. LMS-CP-5510, “Aerospace Systems Change Control within Systems Engineering.”
l. EEE-INST-002, “Instructions for EEE Parts Selection, Screening, Qualification, and Derating.”

P.5 CANCELLATION

None

original signed on file

Douglas L. Dwoyer
Associate Director, R&T Competencies

Table of Contents

1. Introduction

1.1 Background

- LaRC's processes and procedures are managed through the Langley Management System (LMS) in order to deliver a quality product.
- LaRC will deliver products that meet or exceed customer expectations.
- LaRC is committed to reducing the total cost of flight systems' success, from design/development through flight operations, consistent with the vision and mission of the Agency.
- The number of space flight systems activities at LaRC utilize a significant part of the Center's workforce and is expected to increase, especially in planetary exploration and space transportation.
- Success must be achieved under conditions of tight budgets and constrained development schedules. These conditions create an intense demand for skilled, experienced personnel.

1.2 Activities To Achieve Highly Successful Space Flight Projects

There are several activities that will enable more effective and efficient projects. These activities are an integral part to the overall success of the project.

- Co-locating appropriate personnel to enhance work efficiency,
- Increasing interdependencies to reduce overall cost and promote teaming,
- Developing and maintaining state-of-the-art design-and-test tools and test-and-assembly facilities to reduce development time and cost,
- Improving access to key technical personnel to identify and resolve issues early,
- Increasing emphasis on mentoring to properly train personnel,
- Setting up an electronic, mechanical, and optics parts replacement scheme to provide adequate stores,
- Documenting and/or updating processes to standardize project development, and
- ***Documenting flight-proven system design, flight operations, and safety and mission assurance principles to guide project implementation.***

This last activity is the subject of this document.

1.3 Additions/Updates

As technologies develop and design methods improve, additions and revisions will be identified to these principles and passed through the same process as was taken to generate this initial set. The need for updating will be evaluated annually.

1.4 Categorization of the Principles

These principles reflect LaRC standards and are intended to align with Agency standards and processes. The design principles are categorized into the three following sections:

- Section 2 - General Principles
- Section 3 - Detailed Principles
- Section 4 - Flight Operations Principles

1.5 Adherence to Principles

- Proposals responding to Announcement of Opportunities (AO's) shall address exceptions (as known at that time) to these principles at the Project/Experiment Initiative Review (PEIR).
- Project exceptions to the general principles shall be documented, with rationale, in the Project Plan.
- Project exceptions to the detailed principles and to the flight operations principles shall be addressed during the project lifecycle in the appropriate project reviews. The Project Plan will identify the appropriate reviews and how the principles will be addressed in these reviews. The review requirements are established in LMS-CP-5505, “Flight Project and Experiments Review Planning and Implementation in Accordance in NPR 7120.5.”
- Exceptions or changes to any of these principles identified subsequent to the Project Plan approval shall be documented by the project through a waiver. For tracking purposes a summary log identifying all waivers shall be included in an update to the Project Plan.
- All exceptions/waivers to these principles shall be addressed at the Flight Readiness Review (FRR).
- For System Contract/Partnering implementations, the project shall obtain from the Contractor/Partner exceptions to the principles and document these exceptions. Organization of Principles

The principles within each section are listed more or less chronologically as they would be considered and implemented during the course of a flight project implementation. Global principles are listed first; then design planning and requirements, design implementation, verification and validation, and finally flight operations.

1.6 Format of Principles Descriptions

The principles are headed by a bold numbered subject heading, such as “**2.3 Early Design Decisions**” and include a “shall” statement. Some principle descriptions are augmented by a supporting “***Rationale***” and/or an amplifying “***Note***” which are in italics. These statements generally apply to the principle described immediately above them, but in some cases may apply to several of the principles above them.

2. General Principles

2.1 Priorities

2.1.1 The Project shall treat safety of people (project personnel, flight crew, and the public) as the paramount requirement. Hence, safety requirements and compliance thereto shall be shown to not have been compromised in trade-offs against other project parameters.

2.1.2 The project shall apply prudent engineering and risk management decision-making to achieve mission success within the cost and schedule constraints sacrificing performance, if necessary. Consistent with this, the project ordered priorities shall be safety, reliability, cost, schedule, and performance.

2.1.3 The project shall also prioritize/weigh, with rationale, mission/system competing requirements to guide design and implementation trade-offs.

2.1.4 The project shall provide a description regarding how priorities will be used to guide the resolution of technical/programmatic issues as well as guide the design implementation in the appropriate planning documents. (e.g. The Systems Engineering Management Plan)

2.2 Modeling/Simulation

2.2.1 The Project shall use modeling and simulations early and often to develop and evaluate designs. The models shall be realistic by taking into account real mechanical/electrical configurations, intended operational conditions, material properties, etc.

2.2.2 The Project shall document expectations/predictions for the models/simulations used and their fidelity limits.

2.2.3 The Project shall test-validate models/simulations. .

2.2.4 The Project shall assess and compare modeling/simulation outputs with predictions and system requirements.

2.3 Early Design Decisions

Projects shall identify and maintain a "top ten" list of required design decisions and milestones.

Rationale*: It is better to make a few "questionable" decisions that keep the design process moving forward rather than delay decisions to make the design "perfect." Remember, "better is the enemy of good;" hence, avoid the temptation to make the design better if it is already good enough.*

Note*: This principle is enabled by early definition and approval of requirements and capabilities.*

2.4 Design to Requirements/Capability

2.4.1 Mission and system requirements, as well as intersystem capabilities and interfaces, shall be baselined (approved by the project) and a functional design identified that can satisfy the requirements as early as feasible but by project PDR at the latest.

Note: *Desires/goals may be considered if acceptance provides high payoff at low cost/risk or significantly reduces/avoids future cost/risk.*

2.4.2 The design process shall consider existing capability and the cost effective use of inherited (flight and ground) designs, hardware (H/W), software (S/W), systems engineering (SE), etc., as a major cost/risk reduction. Heritage assessment reviews will be performed to validate cost/risk savings when using this approach.

2.4.3 Designs shall use commercial off-the-shelf (COTS) functionality where it is feasible and reduces cost/risk. Especially consider COTS for engineering models (EM) and ground support equipment (GSE).

2.4.4 Particular attention shall be given to past Non-conformance Failure Reports (NFR's) relating to the existing capability or design.

Rationale: *Identifies incompatibilities between previous usage and current project requirements.*

2.4.5 The design process shall consider the use of new concepts/advanced technology when it is needed to meet the priorities, provides or preserves prudent margins, or is identified as a requirement to enable future missions.

2.4.6 New technologies/concepts shall be identified in the project implementation plan with the associated risks addressed. Actions being taken to maximize prospects for success (reducing risk) shall be included. Use of technologies whose assessed maturity is less than TRL 6 shall be justified in the Project Plan.

2.4.7 Operating characteristics and requirements drivers from inherited/existing flight systems elements on the flight operations system design and vice-versa shall be identified in the preliminary design activity and reviewed at the flight system PDR.

Rationale: *To identify requirements feasibility and drivers and to assess intersystem and flight system/ subsystem design compatibility with them so that existing capability and costing assumptions can be validated and later, costly changes will be avoided.*

2.5 Standards

Industry and Agency standards (H/W and S/W) shall be considered in all areas of the design to reduce cost/risk. Where deviation from standards is necessary and risk is consciously accepted, these risks shall be included in the Risk Management Plan.

2.6 Risk -Based Design Trade-Offs and Margin

2.6.1 Trade-offs based on balancing risk shall be used in design/development/mission operations decision-making and be consistent with the project's principle for priorities, particularly safety.

Rationale: *A balanced risk approach improves the prospects for success within technical/programmatic resources. Trade-off studies can be used to identify effective use of programmatic and technical resources in varying combinations, enabling proactive risk management to balance/reduce overall project risk.*

2.6.2 HW/SW trades shall be performed early in the project using risk as a metric.

2.6.3 Design and programmatic resource margin requirements (e.g., mass, power, budget, schedule) shall be established early in the project. The usage of these margins to effectively solve problems and mitigate risk shall be a part of the margin management planning.

2.6.4 The actual usage of the margins shall be assessed and reported against the plan regularly throughout the life cycle. Corrective action shall always be considered when actual usage deviates significantly from plan.

2.6.5 To maintain this balance, the project shall consider accepting, when prudent, the least unsatisfactory trade-off solution for problem resolution.

2.7 Single Failure Tolerance/ Redundancy

2.7.1 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.

Note**:** *Redundancy may be used to provide protection against potential single point failures. Redundancy may be implemented as block or functional redundancy.*

2.7.2 Where block redundancy is used, cross-strapping circuitry shall be subjected to Failure Mode Effects Analysis (FMEA) to demonstrate intended reliability improvements.

Note: *Cross strapping adds significant cost, possible "sneak path" failure modes, and increases system complexity requiring more extensive fault analysis, system and subsystem testing and more test time to acquire operating hours and characterize the cross-strapped configurations.*

2.7.3 A potential single-point-failure exemption list shall be developed (e.g., primary structure).

2.7.4 A list of potential credible single point failures shall be developed, maintained and reported at SRR, PDR, CDR, SAR, and FRR.

2.7.5 The list of accepted potential single point failures shall be communicated to the flight operations team. Particular attention shall be given to those items where the risk mitigation plan requires flight operational actions.

2.7.6 All identified potential single-point failures shall be addressed at the SAR and FRR.

2.7.7 Use of single-string design may be considered if risk can be demonstrated to be acceptable.

Note: *Engineering subsystems are generally made redundant for long missions. Missions may consider single-string designs based on historical failure data, statistical trade studies, design robustness, and consequences of mission failure. Projects that adopt a single-string operational approach for critical events should do so with special attention to the use of functional redundancy and control algorithm robustness. The Project should determine a risk level by SRR including a reliability target to facilitate the design process.*

2.8 Nuclear Materials

The design shall avoid the use of nuclear materials (e.g., radioisotope heating unit, radioisotope thermoelectric generator) unless they are essential to mission viability or overwhelmingly cost-effective.

2.9 Design Fallback Options

2.9.1 Design descope or fallback options shall be identified early in design conceptualization.

Rationale*: High risks (e.g., using new technology) may be carried longer in the implementation if descope options are available.*

Note: *The impacts on the design performance and effort resulting from exercising these options must be understood and acknowledged.*

2.9.2 Trigger events/dates for the descope decisions shall be identified in advance and adhered to.

Rationale*: This facilitates decisions as late as possible while still retaining the benefit of descoping.*

2.10 Safety and Mission Assurance

2.10.1 The project shall plan early in the formulation phase for adequate safety and mission assurance (S&MA) activity, and shall identify the responsibilities of the participating organizations in tailored Safety and Mission Assurance (S&MA) Plans. These plans shall define the project’s implementation of the following :

- Mission Assurance
- Independent Assessment
- System Safety
- Reviews
- Risk Management
- Reliability Engineering
- Quality Assurance
- Electronic Parts Engineering

2.10.2 Mission Assurance shall be integrated and concurrent with the design activity throughout the project life cycle.

2.10.3 Project quality assurance provisions shall flow down to all project acquisitions.

***Rationale**:*

1. *Reflects the S&MA approach to the customer so that mission assurance can be involved in the earliest design decisions.*
2. *Avoids redesign resulting from after-the-fact Mission Assurance reviews and resolves product quality issues as they arise.*
3. *Communicates the mission assurance program with the project and provides acknowledged infusion of S&MA into development processes.*

2.11 Design Margins

2.11.1 Design margin requirements shall be established consistent with design maturity and mission environments and shall consider potential changes due to environment and mission/system design uncertainties and "unknown unknowns."

2.11.2 Design margins shall be robust enough to accommodate design uncertainties and enable design changes with minimal system-wide "ripple effects."

***Rationale**: Robust margins enable design and programmatic trades to be made effectively and rapidly without lengthy studies, thereby preserving programmatic resources (budget and schedule).*

2.11.3 Design margins shall be managed and traded at the highest possible level in the mission or system (e.g., performance-vs.-available power, allocations of timing uncertainties).

***Rationale**: If margins are locally traded, artificial constraints can be created which unnecessarily reduce the system capability to achieve the prime mission/science objectives **OR** cause non-productive work.*

2.11.4 Robust margins in system resources shall be available for flight operations.

***Rationale**: Sufficient margins in system resources such as power, thermal range, telecom, memory, timing, bandwidth, and pointing improves operability by enabling operators to effectively accommodate differences in flight conditions from predicted and by maximizing response capability to anomalies while preserving mission return.*

2.12 System Performance Allocations

2.12.1 The project shall identify and allocate nominal values and uncertainties to the distributed contributors to system performance (e.g., pointing error contributors) as early as possible. Driving system performance contributors shall be identified and included in the project risk assessment.

2.12.2 Estimates of nominal and uncertainty values shall be updated as often as needed and specifically reviewed at major design reviews (e.g., PDR, CDR).

2.13 Combining System Performance Contributors

2.13.1 The approach (e.g., linear sum, root-sum-square, confidence level) for combining system performance contributors' nominal values plus uncertainties shall be defined for each performance measure.

2.13.2 This combining approach shall take into account the dependence/coupling of the contributors, the nature of the uncertainties (systematic or random), and the uncertainty distributions (Gaussian, uniform, etc.).

2.13.3 Specific unallocated margin, relative to the performance requirement, shall be identified and maintained in this combining process.

2.14 Lessons Learned/NASA Alerts

The design shall 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 shall be identified and dispositioned.

***Rationale**: Important lessons can be drawn from past events which have applicability beyond the original event and which can preclude recurrence of faults/failures and enable early and cost-effective changes. Some examples of past troublesome areas are as follows:*

- *Cabling, e.g., wire treatment, open pins, insulation*
- *Power converter design*
- *EEE parts*
- *Deployments (e.g., booms, covers)*
- *Optical system contamination*

2.15 Project Risk Assessments

2.15.1 The project shall perform, with appropriate independent assessment support, a total mission risk assessment at inception of project and in reviews as defined. These assessments shall be documented in the appropriate project planning documents.

***Rationale**: To ensure LaRC and customers are informed of risk to program/project success and to provide independent assessment back to project to enable possible mitigation approaches outside the project's sphere of influence.*

2.15.2 These assessments shall specifically identify and address risks to project and program objectives.

2.15.3 Risk assessments shall specifically include margin assessment as one of the risk metrics.

2.16 Closed-Loop Failure Reporting and Flight Team Awareness

2.16.1 The LaRC electronic NFR System shall be used.(http://nfr-anomaly/login_usage.cfm)

2.16.2 When a prime contractor's system is used, their NFR's shall be recorded in the LaRC NFR system as well.

***Rationale**: Uniformity of describing and reporting problems and consistent reference capability enables cross-project understanding of risks and implications of the issues.*

2.16.3 The project shall establish and use a concurrent engineering process involving the appropriate project team members (e.g., designers; systems engineers; assurance, test and operations engineers) to close problems in a timely and confident manner.

2.16.4 The project manager shall disposition the acceptance of NFR's and address them at the SAR and FRR.

2.16.5 Appropriate NFR's shall be compiled and forwarded routinely to the flight operations team preferably at or before the beginning of Flight-Ground System end-to-end testing.

Rationale*: To make the flight team aware of those pre-launch problems that may pose a significant threat to flight operations activities.*

2.17 Peer Reviews

2.17.1 Projects shall use independent peer oversight/review of subsystems and systems prior to design reviews (PDR, CDR, etc.). Peer reviews shall include intra-system reviews. These reviews shall be implemented using the LMS procedure LMS-CP-5508, "Ad-Hoc Technical Reviews (including Tiger Teams)"..

Rationale*: Peer Reviews provide early detection and correction of deficiencies, and provide periodic assessments of progress against plan. Use of experts from outside the project team improves the activity. Peer reviews allow discipline-specific penetration into the details of design and implementation issues. Reporting the findings to a subsequent project review provides the review board with essential detailed insight otherwise not available in the formal review presentation format.*

2.17.2 PDR and/or CDR shall address the findings and actions from the peer reviews.

Rationale*: Peer reviews properly focus on the adequacy and characteristics of the detailed design of elements of the system. In order to maintain compliance with mission and operations customer expectations, timely independent review of results of the peer reviews against systems requirements, concept of operations, and mission design is necessary and effective.*

2.17.3 Peer Reviews shall be recommended/considered by line management or project as needed to deal with special topics or issues as they arise.

2.18 Testability

2.18.1 The design shall be implemented so that hardware testing, including in-situ troubleshooting activities, can be effectively performed at the subassembly (board), assembly, subsystem and system level.

2.18.2 The design shall enable software testing at unit, module, subsystem test bed, and system test bed levels to incrementally verify functionality/operability.

2.18.3 The software design shall include self-test and built- in test routines to test operation and permit timely fault diagnostics. The design shall include diagnostic/test mode commands capable of operating a subsystem of the overall system in isolation to facilitate ground testing and operations.

2.18.4 The software self-test and built-in test routines shall be removable for flight. If not removable, the test routines shall not cause flight hardware damage or interfere with proper operation of the flight software if inadvertently executed in flight.

2.18.5 The design shall enable "early and often" testing throughout development.

2.19 Accessibility

2.19.1 The design shall provide sufficient accessibility to permit hardware rework/verification in a reliable, efficient manner without adding unwarranted hardware risk.

2.19.2 The design shall avoid the use of "blind" mating of electrical connectors.

2.19.3 Sharp corners or edges shall be avoided in the flight system design.

Rationale*: Precludes injury to personnel, or damage to hardware caused by snagging of garments.*

2.20 Test Beds

2.20.1 The number and type of test beds, including S/W-only test beds, and GSE (H/W and S/W) shall be identified and provided for early in the development plan.

Rationale*: Multiple test beds enable concurrent testing to be done at various stages during the development cycle. Multiple test beds enable a "build a little, test a little" design approach for early software or hardware/software problem identification and resolution. S/W only test beds enable early software and/or flight sequence problem identification and resolution prior to committing to the more expensive and often time-critical use of the hardware system test beds.*

2.20.2 Test bed fidelity shall be maintained. Differences (H/W and S/W) from flight shall be documented and maintained. Simulation models shall be validated by test, using sufficient parametric variation in the simulations to ensure the existence of adequate margins when system-level flight system verification is performed on a test bed.

Note*: During component selection, system engineers should consider the modeling feasibility and effort as extremely important selection criteria.*

2.20.3 The Project shall 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.

2.21 Test and In-flight Protection of Flight Hardware

2.21.1 Flight hardware interfaces with ground handling and test equipment shall be designed with protective overvoltage/overcurrent or overpressure, etc., devices.

Rationale*: Precludes test operator/test equipment or environmentally-induced (e.g., lightning) damage or degradation to flight hardware.*

2.21.2 The system H/W and S/W developers shall provide to the flight operations team a set of operating flight rules including health maintenance rules and rules for life -limiting elements that ensure the health/safety of the flight system.

2.21.3 System developers shall be involved in conducting flight operations particularly in the early operations activities following launch.

2.22 Systems Validation

2.22.1 The project shall establish a plan for demonstrating that the integrated project systems will accomplish the intended mission and effectively satisfy the customer's goals and objectives.

2.22.2 The project shall perform a Mission Design Verification Test (MDVT) to validate the end-to-end capability of the mission systems to accomplish mission objectives.

2.22.3 System Validation shall include the following:

- Establishing that the requirements identified through mission synthesis to the implementing systems, traced down to the lowest levels of implementation, meet customer needs.
- Demonstrating, through the Systems Design Verification activity, the confidence that the requirements are met and the inter-operability of the H/W and the S/W.
- Demonstrating, through end-to-end integrated systems analysis, the acceptable inter-operability, and robustness of the systems,
- Demonstrating, 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.

2.23 Design Verification

2.23.1 The project shall establish a systematic comprehensive system design verification plan showing how all system requirements compliance will be demonstrated.

2.23.2 "Test as you fly and fly as you test" (e.g., using flight sequences, flight-like operating conditions, and the same software functionality) shall be the system verification philosophy. Where testing is not possible, verification shall be demonstrated by independent analyses.

2.23.3 The design verification plan shall at least provide for nominal and off-nominal end-to-end system verifications, environmental verifications, fault protection, flight sequence, and cross-system verifications.

2.23.4 Appropriate system-level stress testing (beyond normal design verification level) shall be performed to determine capability boundaries and demonstrate robustness of the end-to-end systems design in order to assure health/ safety and provide confidence in successful completion of mission critical activities. Stress testing shall consider testing (e.g., single faults that cause multiple-fault symptoms) the occurrence of subsequent faults in an already faulted state, etc.

2.23.5 The design verification plan shall also provide for early system functional and performance verifications. In particular, system level verifications shall 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 shall require a system level electrical "plugs-out" test using the minimum number of test equipment connections.

2.23.6 In addition to the usual real-time data analysis, comprehensive non-real time analysis and trend analysis of test data shall be planned to identify problems and enable early resolution with minimal cost/schedule impact.

2.23.7 Hardware and software verification shall be planned during the formulation phase.

2.23.8 Testing shall be the primary method for design verification. If test verification is not practical or appropriate, other methods such as modeling/simulation using test-verified models/simulations, analysis, and inspection shall be specified and used. Results of verification by simulations and/or analyses shall be independently reviewed.

2.23.9 Verification by visual inspection of mechanical clearances and margins (e.g., potential reduced clearances after blanket expansion in vacuum) shall be performed on the final as-built hardware.

Rationale*: To verify the adequacy of thermal blanket clearances, etc., before and after environmental test, handling, etc.*

2.23.10 Verification of all deployable or movable appendages and mechanisms shall include full-range articulation.

2.24 Use of Engineering or Prototype Hardware

2.24.1 Engineering or prototype models shall be as identical as practical to the flight units in the functionality being tested. When used to validate/qualify a design, the model shall be tested to the appropriate levels for validation/qualification.

2.24.2 If engineering or prototype models are intended to be possible future flight spares, the plan for this usage shall be established early in the design concept development.

2.24.3 To enable use of engineering or prototype models as flight spares, appropriate actions shall be taken to ensure hardware safety, reliability, functionality, and traceability.

2.25 Use of Protoflight Hardware

2.25.1 Protoflight hardware (hardware intended to be flown for which there is no direct qualification heritage) shall be validated/ qualified to the following conditions:

- Thermal - Qualification levels and durations
- Dynamic - Qualification levels but Flight Acceptance durations
- EMC/Magnetics - Qualification levels

Notes: 1. Flight Acceptance is the demonstration that the test item will function within performance specifications under simulated environments expected from ground handling, launch, and orbital operations.

2. Qualification is the demonstration that the test item will function within performance specifications under simulated environments more severe than those expected from ground handling, launch, and orbital operations.

2.26 Critical Hardware Power On/Off Cycling

In-flight routine power cycling of critical hardware for power margin management purposes shall be avoided *unless cycling is essential to mission viability and the risk is demonstrated to be acceptable.*

2.27 Critical Sequence Telemetry/Monitoring

2.27.1 The design shall provide the capability for simultaneous real-time transmission and on-board storage of mission critical sequence data. Stored critical data shall be protected from loss in the event of selected anomalies (e.g., transient power outage) and shall be transmitted to Earth as soon as practical.

2.27.2 Mission critical events (e.g., Launch Vehicle separation, deployments, etc.) and deployables verification shall be available via real-time telemetry.

2.27.3 The flight software shall have telemetry monitor (TMON) capabilities. TMON are capable of autonomously detecting an out-of-limit condition and autonomously executing appropriate routines to safe the payload/spacecraft.

2.28 Earth Orbital Debris

2.28.1 Orbital debris safety considerations shall be addressed during the project formulation phase and during the implementation phase.

2.28.2 Orbital debris from launch vehicles, spacecraft, instruments or components thereof (e.g., launch vehicle 2nd or 3rd stages, instrument covers) shall be limited, as much as practical, by employing prudent design and flight operations techniques as appropriate.

- The design and flight operations shall employ debris-limiting options (e.g., propellant depletion burns, cover release inhibits) considering normal and off-normal operations and certain anomalous events (e.g., explosions, breakups, or collision with other debris).
- Identification of orbital debris sources, potential hazards, and a debris-limiting assessment shall be presented at the SRR. Functional design implementation shall be reviewed at the project PDR and finalized at the CDR.

Rationale*: Limit the proliferation of debris that may be a safety threat to personnel or space vehicles (current and future) generated by orbital debris.*

2.28.3 Earth orbiting spacecraft shall be designed (wherever possible) with capability to be de-orbited reliably at the end-of-mission.

2.29 Telecommunication Telemetry/Command Capability

Telemetry and command capability shall be available throughout the mission in normal orbit/cruise pointing attitude, and during special orbit/cruise phase mission/system activities

Rationale*: To provide "real-time" monitoring of activities and enable ground contingency commanding, if necessary.*

2.30 “Keep-it-simple” Design Philosophy

2.30.1 Designs shall employ a “keep-it-simple” philosophy (i.e., straight-forward designs) to reduce risk/cost and to enable easy implementation, design verification, and flight operational usage (e.g., where appropriate, passive antenna coupling-vs.-active switching).

2.30.2 Use of “complex” design implementations shall be avoided. Added complexity shall be justified to be essential to meet mission requirements/constraints.

Rationale*: To maximize the prospects for safe and reliable operation.*

2.31 Hardware/ Software System Design and Verification

2.31.1 Standards shall be utilized in defining HW/SW and SW/SW interfaces between the flight systems and the ground, between flight systems, and within a flight system (e.g., CCSDS for telemetry and command).

2.31.2 System/mission requirements shall be traceable to the project-level requirements, and detailed requirements on hardware and software elements, and interfaces between them, shall be traceable to the system/mission requirements.

Rationale*: To ensure completeness & correctness of critical requirements, in order to use requirements to accomplish software and system validation.*

2.31.3 Mission scenarios shall be generated early and used to enable effective hardware/ software functionality allocation. They shall be maintained current and used to guide the design, integration and test activities at all levels.

2.31.4 The number and type of interfaces employed in the design of the flight software shall be minimized.

2.31.5 Test/diagnostic code shall be designed and incorporated into the software early so that problem resolution can be done rapidly and easily at element and flight system level and can adapted by the flight operations team.

2.31.6 Fault case issues shall be addressed and solutions incorporated into the design as early as practical during the design cycle. Fault protection software shall be specified in the systems engineering process to handle all credible flight system single -fault scenarios.

2.31.7 Prior to computer design/procurement, analysis shall be employed to estimate the amount of throughput and memory required to meet the project needs. Procured or designed processing components shall exceed estimated requirements by at least a factor of 4.

2.32 Mandatories List

No later than nine (9) months before launch, the project shall develop and maintain a prioritized list specifying the mandatory assembly, tests, launch, and mission operations tests/products that must be completed to commit to the launch. Changes to the list or test/product shortfalls shall be reviewed and approved by the project manager.

Rationale*: Permits the project to focus on the essential work and make the most effective use of personnel, schedule, and budget resources.*

3. Detailed Principles

3.1 System Mass and Power Margins

Because of the ambitious nature (technical and programmatic) of LaRC space flight endeavors, aggressive balanced risk management is necessary to enable success. Therefore, it is prudent to have ample mass and power resources to account for and accommodate uncertainties and expected growth. Furthermore, ample mass and power resources in conjunction with ample funding resources provide flexibility to resolve developmental and operational issues, and enable timely, balanced risk management decisions without having to perform time-consuming trade studies to micro-manage every kilogram and watt. For example, projects can use funding to mitigate mass and/or power growth, or use both funding and mass to mitigate power growth, or use mass and power to preserve budget and schedule.

The detailed design principles for mass (3.1.1) and power (3.1.2) margins are based on a review of actual growth histories for several JPL flight projects. These data suggest that total mass and power growth from knowns and unknowns (items that become known only as the design is being implemented) ranged from 20% to 48% with most in the range of 25% to 40%. Factors affecting growth included mission/system design changes, design complexity, amount of inheritance, amount of new technology/concepts, quality/fidelity of early estimates, and available funding.

A mass metrics versus design life-cycle maturity chart (Figure 1) is provided to graphically illustrate margin, current best estimate (CBE), allocations and growth. A similar chart can be generated for power, etc.

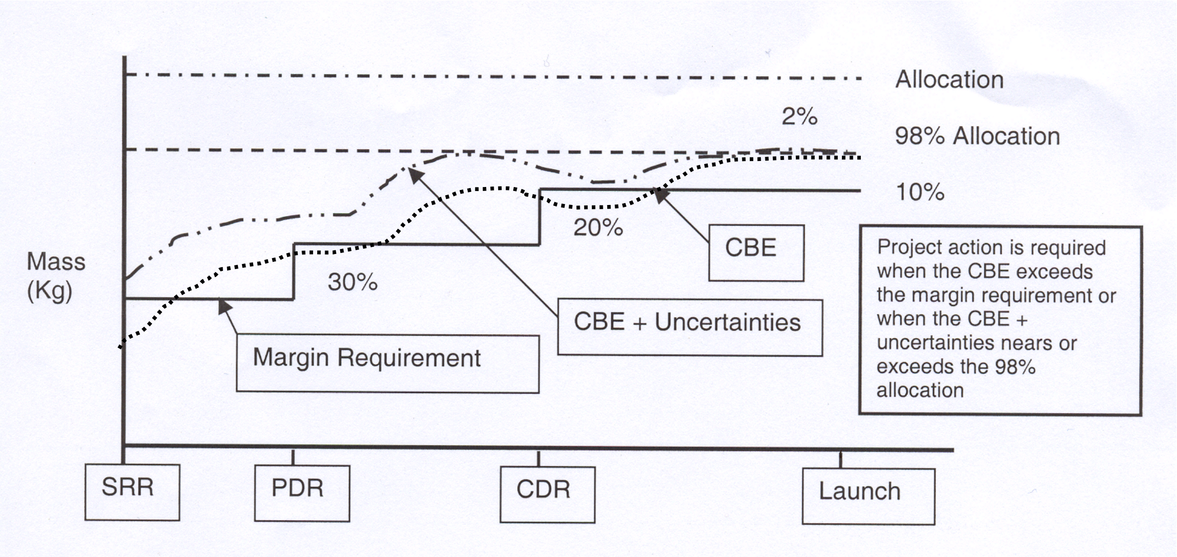


Figure 1

3.1.1 Mass Margins

3.1.1.1 Definitions:

Margin = Allocation - Current Best Estimate (CBE)

% Margin = (Margin X 100)/Allocation

- Allocation is defined as the capability from the launch vehicle for missions and from the spacecraft for instrument/payloads.
- CBE is defined as the best estimate taking into account everything known.
- To improve the prospects for meeting the actual allocation, a reduced allocation may be used in the above management algorithm that subtracts a reserve of a few percent (e.g., <5%) of the allocation as a margin management reserve.

3.1.1.2 The above %-margin definition shall be used by all projects in both the Formulation and Implementation phase.

3.1.1.3 Positive Margins shall be maintained throughout the development cycle.

3.1.1.4 The following algorithm, based on mass growth history, shall be used to estimate potential mass growth:

New designs shall use **30%** *or more* growth from the SRR depending on the nature, maturity, amount of new technology/ concepts, and complexity of the design.

Inherited designs shall use **15%** *or more* growth from the SRR depending on the outcome of inheritance reviews.

Inherited hardware shall use **10%** *or more* growth from the SRR depending on the outcome of inheritance reviews.

Inherited "use-as-is" hardware shall use **2%** growth from the SRR if hardware is totally known to be without change, and is "build-to-print." Any change to these conditions should be evaluated and a larger growth percentage applied.

3.1.1.5 Experience indicates there will likely be significant growth to deal with knowns and unknowns in new designs. Adequate margin shall be provided to accommodate growth. Based on the system level of the specific LaRC project, systems at the spacecraft level, systems at the payload level, or systems at the major instrument level shall have a mass margin of at least 30% at the SRR, 20% at PDR, 10% at CDR, 5% at beginning of assembly, integration and test, and 2% at launch or as set by the project manager and documented in the Project Plan.

3.1.1.6 Required margin curves shall be generated for mass to assess status throughout the design life cycle (e.g., SRR, PDR, CDR); the beginning of assembly, integration, and test; and launch. Margins can decrease as design maturity increases (less uncertainty).

3.1.1.7 For systems at the spacecraft level, mass shall account for on-board propellants. The propellant load shall be sized to provide the required delta velocity for the total mass allocation.

3.1.1.8 Mass CBE's and mass growth shall be reported and compared with the required margin curves to assess margin status periodically (at least quarterly) and at Implementation Phase design reviews. Mass growth estimates shall be combined in a linear, RSS, or combination thereof depending on dependence/ coupling. Monthly mass reporting shall be considered where appropriate (e.g., to the CPMC).

3.1.1.9 Significant deviations from the mass margin requirements shall be accompanied with rationale and recovery options/impacts.

3.1.2 Power Margins

Definitions:

Margin = Allocation - CBE

% Margin = (Margin X 100)/ Allocation

- The above % margin definition shall be used by all projects in both the Formulation and Implementation Phases.
- Allocation is defined as the capability from the power source. Where the capability degrades with mission duration, the allocations should be based on specified (end-of-mission) performance
- CBE is defined as the best estimate taking into account everything known.
- To improve the prospects for meeting the actual allocation, a reduced allocation may be used in the above management algorithm, which subtracts a reserve of a few percent (e.g., <5%) of the allocation as a margin management reserve.

3.1.2.1 Positive margins shall be maintained throughout the development cycle.

3.1.2.2 The following algorithm shall be used to estimate design growth:

> **New designs** shall use **30%** *or more* growth from the SRR depending on the nature, amount of new technology/ concepts, maturity and complexity of the design.
>
> **Inherited designs** shall use **15%** *or more* growth from the SRR depending on the outcome of inheritance reviews.
>
> **Inherited hardware** shall use **10%** *or more* growth from the SRR depending on the outcome of inheritance reviews.
>
> **Inherited "use-as-is" hardware** shall use **2%** growth from the SRR. Any change to these conditions should be evaluated and a larger growth percentage applied

3.1.2.3 Experience indicates there will likely be significant growth to deal with knowns and unknowns. Adequate margin shall 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 SRR, 20% at PDR, 15% at CDR, and 10% at the beginning of Assembly, Integration, and Test.

3.1.2.4 Required margin curves shall be generated for power to assess status throughout the design life cycle (e.g., SRR, PDR, and CDR). Margins can decrease as design maturity increases (less uncertainty).

3.1.2.5 Power CBE's and power growth shall be reported and compared with the required margin curves to assess margin status periodically (at least quarterly) and at implementation phase design reviews. Power growth estimates shall be combined in a linear or RSS or combination thereof depending on dependence/coupling. Monthly power reporting shall be considered where appropriate (e.g., to the CPMC).

3.1.2.6 Significant deviations from the power margin requirements shall be accompanied with rationale and recovery options/impacts.

3.1.2.7 At launch, there shall be at least 10% predicted power margin for mission-critical, orbiting or cruise, and safing operating modes to accommodate in-flight operational uncertainties (e.g., unexpected increases in electrical load consumption; different than pre-launch planned usage profile; and/or less than pre-launch expected power source output), improve the prospects for successful completion of mission critical activities, and reduce the likelihood of an under-voltage fault condition.

3.2 Flight Software Margins

3.2.1 Prior to computer design/procurement, analysis shall be employed to establish margins for critical performance resource parameters such as CPU speed, control cycle rates, interrupt rates and durations, communications bandwidth, random access memory (RAM), and erasable programmable read-only memory (PROM and EPROM). Analysis results are documented as the initial CBE. As flight software development progresses, analysis shall be repeated to update CBEs for comparison to computer capability. A development shall observe the following experience-based guidelines for margin at critical development milestones:

- At computer selection (SRR or PDR), total capability to be 400% of CBE
- At CDR- 60% margin
- At launch - 20 % margin[1]

where:

Margin = Total Capability – CBE

%Margin = [100 x (Total Capability-CBE)]/(Total Capability)

3.2.2 The flight software shall 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.

3.2.3 CBE’s for identified margins shall be tracked continuously and reviewed at least quarterly as well as at PDR; CDR; Start of Assembly, Integration, and Test; and Launch. Margins shall be re-computed in conjunction with proposed significant design changes.

3.2.4 Significant deviations from the margin requirements shall be accompanied with rationale and recovery/options impacts.

3.2.5 Flight software shall accommodate both nominal hardware inputs (within specifications) and transient off-nominal inputs from which recovery may be required.

3.3 Power-On Reset (POR) State/Toggle Commands

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

[1] To accommodate post-launch fixes, new capabilities, and to maintain adequate in-flight operating margins

3.3.2 A POR occurrence shall be unambiguously identifiable via telemetry.

3.3.3 To reduce uncertainty of knowledge of spacecraft/payload/instrument state, toggle commands shall be avoided.

3.4 Fault Protection/Flight Team Commandability

The fault protection system design shall 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.

3.5 System Fault Recovery State Response

3.5.1 Following a fault condition during non mission-critical orbiting or cruise periods, the flight protection response shall, at a minimum, autonomously configure the spacecraft to a safe, quiescent, ground-commandable state, transmitting at least an RF carrier downlink signal.

3.5.2 During critical mission activities (e.g., launch, orbit insertion), the flight fault protection response shall autonomously re-establish the needed spacecraft functionality to permit safe, reliable, and timely completion of the mission critical activity.

3.6 Slosh Dynamics/ Mass Properties

The systems effects of propellant-slosh dynamics and other sources of variability in spacecraft or payload system-level mass properties shall be accounted for when applicable. In particular, the effects on stability, pointing accuracy, and fault protection shall be addressed. Methods of positive mass property control (e.g., propulsion latch valves, trim orifices) shall be incorporated into the design to preclude unacceptable fluid migration or mass property change.

3.7 Information System Design and Margin - Data System and Telecommunications

The information system and telecommunication system design shall 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.

3.8 Data System

3.8.1 To meet limited tracking pass demands (e.g., Deep Space Network), the information system design shall consider significant use of data editing, data compression, and improved data encoding techniques to meet downlink telemetry data requirements.

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

3.8.3 The information system design shall use the *minimum* number of normal-operations data modes to meet the science/engineering requirements. Acceptable sub-optimum return shall be considered, particularly if cost/risk can be significantly reduced.

3.8.4 The information system design shall use the *minimum* number of normal operations telemetry formats to meet the mission science/engineering requirements. Acceptable sub-optimum return shall be considered particularly if cost/risk can be significantly reduced.

3.8.5 The information system design shall have engineering emergency data modes and formats (measurements) for diagnostic use. A hierarchical measurement approach shall be used so that assessment of spacecraft/payload/instrument health/safety can be rapidly attained.

3.8.6 The information system design shall provide adequate telemetry data to rapidly assess health status under *normal and faulted* operations. Special consideration shall be given to providing increased telemetry instrumentation for mission-unique or other sensitive functions.

3.8.7 The information system design shall 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.

3.8.8 The information system design shall be capable of passing engineering data through more than one downlink stream.

3.9 Telecommunications Design and Margin

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

3.9.2 To reduce spacecraft mass and power demand, the Earth downlink shall be designed using the lowest practical power-gain product that meets the mission information return and quality requirements with appropriate margin consistent with the mission (and Deep Space Network) capabilities and tracking coverage.

3.9.3 Telecommunication equipment antennas and ancillary hardware shall be the minimum needed to meet the mission and system telecom requirements with acceptable risk and operating margin.

3.9.4 The spacecraft uplink shall be designed to accommodate an S-band or X-band carrier frequency. The spacecraft downlink shall accommodate S-, X- or Ka-Band carrier frequencies. Uplink and downlink frequency allocations are subject to approval by the National Telecommunications and Information Administration (NTIA) as outlined in Chapter 10 of the NTIA Manual of Regulations and Procedures for Federal Radio Frequency Management. The LaRC spectrum manager shall be consulted early in project formulation to identify potential spectrum issues and to help with the spectrum allocation process.

3.9.5 At implementation start, nominal link margins shall be at least 6 dB. Links with extreme geometry conditions, surface-to-orbit links, or surface-to-surface links shall consider 10 dB or more margin depending on the nature, complexity, and scope of design uncertainties.

3.9.6 During implementation, margins shall be probabilistically defined using appropriate statistical combinations of link parameter tolerances. Link margins shall be reported at PDR; CDR; start of Assembly, Integration and Test; and Launch.

3.9.7 The telemetry system end-to-end design shall 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.

3.9.8 The design shall permit simultaneous command/telemetry capability using the same antenna or similar coverage antennas.

3.10 Thermal Design and Margin

Thermal Control Design Margin is the difference between the flight-allowable temperature range and the range between the worst-case hot and cold predicted temperatures. Worst case is that combination of realistic thermal extremes that produces the maximum hot and minimum cold predicted temperatures.

3.10.1 General

3.10.1.1 Thermal design shall be tailored to the specific applications of the mission with consideration for both equipment reliability and temperature/performance interactions.

3.10.1.2 Passive thermal design/approaches shall be used where practical. Active, complex thermal control design shall be avoided whenever possible.

3.10.1.3 The system thermal design shall control the subsystems to within the allowable flight temperature ranges.

3.10.2 Thermal Design Margin

3.10.2.1 The design shall have adequate (as described below) thermal design margin to ensure that there is no credible thermal threat to hardware when operating under normal conditions.

3.10.2.2 Bus electronics (at the mounting or thermal control surface for the specified assembly) and spacecraft mechanisms shall be qualified (by testing) for -35°C to +75°C or flight-acceptance temperature limits extended by -15°C and +20°C, whichever is greater.

3.10.2.3 For credible abnormal conditions resulting from anomaly-induced power dissipation and/or off nominal sun attitude conditions, the thermal design shall maintain temperatures within flight-acceptance limits extended by +/- 5°C (acceptance temperature range).

3.10.2.4 For non-credible, but plausible, conditions the thermal design shall maintain temperatures within flight-acceptance limits extended by -15°C, and + 20°C (i.e. qualification/protoflight levels).

3.10.2.5 The thermal design shall keep piece-part silicon junction temperatures less than 110°C (assuming a mounting surface temperature of 70°C) for the planned circuit design and packaging scheme. Higher junction temperatures may be considered where risk is shown to be acceptable or permitted by other technologies (e.g., GaAs).

3.10.2.6 Except for detectors, optics, and other instrument-unique hardware, the payload/ instrument electronics shall be designed to the spacecraft bus electronics requirements.

3.10.2.7 Optics, detectors, and other unique hardware shall be designed for allowable flight temperature limits extended by -15°C and +20°C. Margins may be tailored to specific applications based on required operating temperature ranges of sensitive elements.

3.10.2.8 Thermal Cycling

- Electronic hardware design shall be capable of surviving power on-off temperature cycling and/or solar exposure cycling of three times the number of worst-case expected mission cycles with worst-case flight temperature excursions. Prior to having a mission estimate, the equivalent of 10,000 cycles with a 15°C delta-T for new/inherited design hardware shall be used.
- Mechanical hardware design thermal cycling profile shall be tailored for the specific application.
- Flight hardware thermal cycling shall be minimized to preclude the risk of damage.

Rationale: *Thermal cycling has been implicated as a major contributor to faults/problems.*

3.11 Propulsion Design and Margin

3.11.1 Propellant tank volume shall be sized to accommodate the nominal mission based on the required deterministic and statistical delta velocity needs (based on the total mass allocation) and appropriate ullage.

3.11.2 Statistical delta-velocity estimates shall be based on 99% probability.

3.11.3 Propellant load estimates shall be based on specification minimum value I for engine/thruster and allocated spacecraft/payload system mass.

3.11.4 Tanks shall meet the appropriate pressure vessel design and safety margin requirements under worst-case conditions.

3.11.5 Safe and reliable operation of propulsion subsystem components (e.g., valves, thrusters) shall be demonstrated by tests over a range of conditions that envelop flight operations expectations with appropriate margins (e.g., feed pressures, flow rates, mixture ratios, high voltages).

3.11.6 A component cycling usage margin of 50% or more beyond the worst case mission use shall be demonstrated based on the hardware heritage, prior mission use, or qualification testing. Margin shall be reported at PDR, CDR, and start of Assembly, Integration and Test.

3.11.7 Hardware shall be thermally controlled to remain safely (>10° C) above propellant freezing temperature whenever the hardware is in contact with propellant or propellant vapor.

3.11.8 Hardware that will come in contact with propellant vapor shall be thermally controlled over the entire mission to remain safely (>10° C) above the temperature at which propellant condensation will occur.

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

3.11.10 Gas regulators (single or series redundant) shall be used to provide long-term isolation of pressurant from the propellant tank.

3.12 Prime Power Distribution/Switching and Margin

3.12.1 Power System Grounding/ Fault Tolerance - The prime power distribution hot and return lines shall be DC-isolated from spacecraft chassis by at least 2 K-ohms.

Rationale: *Ensure that a single-fault short to chassis anywhere in the distribution system between the power source, electronics, and the user loads does not pose a catastrophic failure.*

3.12.2 Load Removal - Prime power on/off switching of electrical loads shall be done by “simultaneously” switching both hot and return sides.

Rationale: *Ensure total load removal (no possible ground return sneak paths) in case of power-related faults.*

3.12.3 Surge Control/ Load Removal - Power interfaces shall be implemented with in-rush current surge suppression protection and with load removal capability to “clear” a load fault.

3.12.4 Critical/ Non-Critical Load Selection - A critical and non-critical prime power bus shall be considered. Hardware power bus assignment (critical or non-critical) shall be consistent with time critical mission load requirements and maintaining spacecraft safety and ground commandability.

Rationale: *It is prudent to provide the maximum power margin practical post-power fault state for normal orbit or cruise operations.*

3.13 Power Converters

3.13.1 Subsystem off-the-shelf power converters shall be assessed to ensure compatibility with application and surrounding circuitry.

Rationale: *Power converter designs differ in their detailed signatures (ripple, spikes, transients, etc). Assessing sensitivity of user circuits to these details early can preclude costly problems later.*

3.13.2 Subsystem power converters shall be capable of operating via an externally-supplied synch frequency signal or in a free-running mode near the synch frequency.

Rationale: *To minimize EMI effects.*

3.14 Interface Circuit Margins

At the start of the Implementation Phase, there shall 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 shall be reported at project PDR, CDR, and start of Assembly, Integration and Test.

3.15 Battery Energy Margin

3.15.1 At the start of Implementation Phase, the design shall have 40% or more energy margin (depending on new or inherited hardware/designs) assuming an allowable depth-of-discharge of 40% and CBE of electrical load demand including losses. Energy margin shall be managed and reported similar to power margin.

3.15.2 For solar array missions, battery capacity requirements shall account for nominal launch/array deployment to orbit or cruise operational conditions as well as appropriate margin for ground and/or space flight anomalies and mission-critical modes.

3.16 Short Term Transient Energy Demands

The design shall consider capacitor bank energy storage to accommodate short-term large peak step loads, (e.g., propulsion valve actuation).

3.17 Pyro Design and Firing Margins

3.17.1 The design shall have the capability to guarantee firing up to 6 NASA Standard Initiators (NSI's) simultaneously under worst-case conditions (temp, voltage, etc.)

3.17.2 Pyro circuits shall incorporate appropriate current limiting to control maximum circuit current flow.

3.17.3 The design of firing circuits shall avoid simultaneous arming of multiple functions without separate independent protection.

Rationale*: To avoid spurious unplanned pyro events caused by planned firings or other transient effects.*

3.17.4 At implementation phase start there shall be 30% margin on the spare pyro firing circuits including cabling and connector pins. Circuit margin shall be reported at PDR, CDR, and start of Assembly, Integration, and Test.

Rationale: *To accommodate late-identified needs with minimum cost and schedule impact*

3.18 Electrical Grounding and Interfacing

3.18.1 Grounding and interfacing shall be implemented in the electrical and mechanical design (including packaging) to minimize EMI. The grounding and interfacing design shall provide the following:

- An equipotential spacecraft/payload/instrument, and “Faraday” cage where needed,
- Low conducted and radiated emissions,
- High transient noise immunity on circuitry, and
- Prevention or minimization of external and internal electrostatic discharge (ESD).

3.18.2 A static bleed resistive path using a 1 M-ohm or greater resistor shall be provided in each assembly from circuit return to the assembly structure.

Rationale: *To prevent charge buildup during periods when the assembly is not mounted to the spacecraft.*

3.18.3 Structure or shields shall not be used for the primary circuit return path. Wires shall be used.

3.18.4 Each subsystem ground tree (i.e. power converter secondary) shall have a local single point DC ground to chassis via the shortest practical wire length.

3.18.5 All non-coaxial interfaces shall 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.

3.18.6 High current, high di/dt and dv/dt interface wires shall be appropriately shielded/grounded. Furthermore, pyro and power interfaces shall be physically separated from signal interfaces as much as practical (e.g., different routing and separate connectors).

3.18.7 Inductive loads (e.g., valve coils) shall be equipped with back-EMF transient suppression.

3.18.8 Space-exposed or "spacecraft-buried" ungrounded conductors shall be demonstrated to not pose an ESD disruption or damage threat. There shall be no ungrounded (floating) conductor >15 cm in length.

3.18.9 Functions that pass through external connectors (e.g., umbilical, direct access) shall be protected in the event of inadvertent connection of any conductor to any other conductor and chassis.

3.18.10 Electrical signals (e.g., data, timing, power, circuit returns) that use flexible cable or that cross mechanical interfaces shall be immune to transient signal interruption.

***Note**: The amount of transient protection depends on the function and sensitivity of the circuits involved.*

3.18.11 Power hot, return, and chassis functions shall 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 shall receive special engineering review/oversight particularly in designs where the prime power, circuit return, and spacecraft chassis are in close proximity.

3.18.12 Electrical interfaces passing through cable cutter separation devices shall be dead-faced prior to actuation of the device (e.g., signal and power interfaces) shall be unpowered.

3.19 Structural Design and Margin

3.19.1 Where cost effective (e.g., not driving mass to the extent that a new launch vehicle is required), the primary structure shall be designed with high safety factors (>2.0 ultimate).

3.19.2 Static load testing shall be required for all primary structures as a part of qualification and to demonstrate margin.

3.19.3 Design shall consider using the most cost-effective lightweight materials to reduce mass as long as they are compatible with other design requirements (e.g., thermal, electrical and safety requirements).

3.19.4 Secondary structure design shall meet the load values from the mass/acceleration curve or test to the flight environments with appropriate margin.

3.19.5 The integrated design of structure, deployed appendages, and the attitude control response shall preclude/minimize possible interactions caused by lower order modal frequencies.

3.20 Force/Torque Margin

3.20.1 Mission critical deployables design (e.g., covers) shall demonstrate a margin of at least 100% under worst-case conditions, particularly for cold, stiff cable bundles, and considering vacuum-versus-air and coefficient of friction effects.

3.20.2 Mission-critical separations design (e.g., launch vehicle, payload release) shall demonstrate a margin of at least 100% under worst-case conditions.

3.20.3 Mission critical mechanisms and actuators design shall demonstrate at least 100% margin for the range of motion at the end-of-life conditions under worst-case conditions including restart from any position within the range of motion.

3.20.4 "Helper" springs shall be used to assure first motion separation of surfaces where fraying/fretting is possible. "Helper" springs shall also be used to provide for guaranteeing latching of deployed elements.

3.20.5 Margins shall be reported at PDR, CDR, and start of Assembly, Integration, and Test.

3.21 Radiation Design Margin (RDM)

***Note:** RDM is a design factor to be applied in the design specification of electronic parts and part application design. **It is not a reserve** or other resource that can be used up during the design*

3.21.1 RDM is defined as (Electronic Part Capability)/(Electronic Part Expected Local Environment)

3.21.2 RDM shall be calculated based on the CBE plus ***reasonable*** margin to accommodate uncertainties for space environment, transport modeling, and part capability.

Notes:

- *Shielding to an RDM of 2 (traditional goal value) is required at the end of the nominal mission unless the project can demonstrate acceptable risk with lower margin.*
- *Circuit design margins are currently calculated including the combined effects of radiation, temperature, aging, voltage variations, etc. Voltage and temperature are major contributors.*
- *Voltage 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.*
- *Where spot shielding of a component is to be applied, an RDM of 3 is required to account for greater modeling uncertainties.*

3.22 Graceful Degradation

The design robustness shall 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

***Rationale:** To reduce possibility of catastrophic mission loss or major mission degradation.*

3.23 Configuration Design and Fields-of-View (FOV) Interactions

3.23.1 The configuration design shall provide an appropriate amount of additional clearance beyond nominal specified FOV's to preclude/minimize obscuration effects (e.g. to sensors, antennas, and thrusters) caused by structural elements, blankets, booms, covers, etc.

3.23.2 Stray-light input shall 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).

3.23.3 Thruster or external venting plume impingements shall be precluded/minimized.

3.23.4 RF antenna pattern distortion effects shall be precluded/ minimized.

3.24 Interface Commonality

3.24.1 The system design shall use a common electrical interface approach and circuits to reduce interface designs and protocols.

3.24.2 The system design shall minimize the number and type of interface approaches/circuits used.

3.24.3 The system design shall 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).

3.25 Reliability Analyses/ Design Confidence

3.25.1 Mission/system-level fault tree analyses (FTA's) shall be performed and maintained/updated throughout the project life cycle. The most recent FTA shall be presented at SRR, PDR, CDR, and SAR.

3.25.2 The design shall be assessed for robustness through a program of analyses tailored from the Space Product Assurance, LPR 5300.1, “Space Product Assurance,” or Contractor/Partners equivalent, including part parameter data from available databases and derating guidelines. Analysis/test types to be performed shall include the following:

- Worst-case circuit analysis and voltage-temperature-frequency margin testing (where it is feasible and prudent) to demonstrate performance margin.

  FMEA at the system/subsystem functional block diagram and interface levels to identify potential critical single failure points. (Failure Modes Effects/ Criticality Analyses (FMECA's) are generally applied to electronics and electronic functional interfaces; subsystem mechanical Fault Tree Analyses (FTA’s) are generally applied to devices and mechanisms.)
- System interface circuit, functional, and fault analyses (mechanical, thermal, etc.) to demonstrate that faults in one subsystem/system will not propagate or functionally degrade other subsystems.
- Parts stress analyses to verify margins.

3.26 Electronic Parts Usage

3.26.1 General

3.26.1.1 Appropriate derating of parts shall be incorporated in electronics design utilizing EEE-INST-002, “Instructions for EEE Parts Selection, Screening, Qualification, and Derating.”.

3.26.1.2 The availability and cost/risk effectiveness of grade-one parts shall be considered before COTS parts become the design baseline.

3.26.1.3 An early design parts list review shall 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

3.26.1.4 The root cause of electronic parts failures shall be determined.

Rationale: *Avoids repeating same or related failure, and develops effective and efficient corrective action that addresses underlying cause.*

3.26.2 ASIC's and FPGA's

3.26.2.1 Mixed signal (digital and analog) ASIC’s shall be considered to meet packaging and power constraints/objectives.

3.26.2.2 ASIC design shall develop behavioral and hardware description models to capture implementation of system design specifications and evaluate performance.

3.26.2.3 Test vectors shall 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.

3.26.2.4 Functional tests shall be performed with simultaneous digital, analog, and mixed signal circuitry to assess interactions as well as separate tests on each portion of the ASIC.

3.26.2.5 Analog, digital, and mixed signal ASIC’s shall be modeled or simulated and compared with test data.

3.26.2.6 Analog and digital ASIC’s shall be wafer-probed at room temperature and at maximum rated operating temperature.

3.26.2.7 Margins shall be maintained for the allocation of gates to implement an ASIC application. Depending on the complexity and maturity of the design, margins shall be at least 15 percent at CDR.

3.26.3 FPGA/ ASIC Transient Operations at Power Turn-On/ Turn Off

Precautions (e.g., time-out) shall be taken to prevent adverse effects due to the unpredictable logic states of FPGA's and ASIC's, which can occur at power-on and power-off.

Rationale: *During power turn-on or turn-off, FPGA's /ASIC's may be in unpredictable logic states for several 10's of milliseconds.*

3.27 Synchronous/ Asynchronous Digital Design

3.27.1 Synchronous design shall be used for digital logic to guarantee the sequence of logical decisions and the validity of data transfer.

3.27.2 The synchronous design of ASIC or FPGA shall 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) shall be constrained both for place, route, and test vector simulation.

Note: *Asynchronous design may be used if techniques are employed and demonstrated to provide guarantees for sequence verification and validation to the same confidence level as used for a synchronous design.*

3.28 Systems Safety

System safety analyses, inspections and tests, and required reports shall be performed according to the guidelines and requirements of the Space Product Assurance, LPR 5300.1. These may include the following:

- A preliminary hazard analysis in support of preparation of System Safety Plan
- A Safety Compliance Data Package
- Safety tests and/or inspections and Facility and Operational Safety Surveys

3.29 Environment Compatibility Verification

Environmental design assessments and verification tests shall be performed to verify the design against the specified environment. These shall be performed at the unit and system level considering the requirements and guidelines of the Space Product Assurance, LPR 5300.1. Such analyses and tests may include the following:

- Analyses of Single Event Effects (SEE), micrometeoroid, pressure profile, magnetic fields, etc.
- Unit-level qualification-level random vibration, pyro, thermal, EMC; and acceptance-level random vibration and thermal
- System-level/protoflight random vibration and/or acoustic, pyro shock, thermal vacuum, EMC

3.30 Electronics Minimum Operating Time

A minimum power-on operating time shall be established for all electronics as follows:

- Unit level prior to system integration -- each electronic assembly, including each side of a block-redundant element, shall have at least 200 hours operating time.
- System Level prior to launch -- each single-string electronic assembly shall have 1000 hours operating time. Each side of a block-redundant element shall have at least 500 hours operating time with a goal of 1000 hours.

3.31 Quality Assurance Verification and Validation

3.31.1 LaRC source QA provisions (LPR 5300.1) shall be provided for critical processes/products and strategically applied to high-risk suppliers.

3.31.2 Analyses, inspections, and/or tests shall be performed to ensure that the as-built product is consistent with the as-designed Baseline Configuration.

3.31.3 Quality assurance provisions, as defined in the project QA Plan, shall be implemented throughout the Assembly, Integration, and Test processes. Such provisions may include the following:

- Working proactively in the safety and contamination control activity to ensure hardware integrity.
- Providing configuration support for test and flight software.
- Assuring that project documentation requirements are met.
- Conducting a physical verification of all hardware to ensure that it meets the workmanship, CM, and other project requirements.
- Witnessing critical operations.
- Maintaining spacecraft/payload/instrument configuration log.

3.32 High Voltage Power Supply Controls

High voltage power supplies shall have at least two (2) independent and separate controls to activate/deactivate high voltage to assure that no single fault/command can result in a high-voltage state, which may result in risk to personnel or hardware or be a mission safety hazard.

4. Flight Operations Principles

4.1 Operability

4.1.1 The flight systems and flight operations design shall be developed concurrently to enable cost-effective end-to-end operations.

4.1.2 The flight systems shall consider methods to reduce operational complexity and interdependencies (e.g. require less calibrations, provide more on-board closed-loop control, provide robust technical margins, provide more autonomy).

4.1.3 Operability design trades conducted and attributes incorporated shall be identified at the flight systems SRR, PDR, and CDR.

4.2 Flight Operation Sequences

4.2.1 Flight sequences shall 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 shall be tested prior to flight use to demonstrate safe, reliable functionality, and acceptable margin *OR* shall be approved by the project manager.

4.2.2 All flight sequences shall have been tested on a high fidelity flight-like system test bed and all anomalies dispositioned prior to sequence uplink transmission.

4.2.3 Standardized sequencing techniques shall be used for repetitive sequencing activities to reduce cost and risk.

4.2.4 For mission time-critical sequences (e.g., launch, orbit insertion), the driving design requirement shall be safety and reliability even at the expense of reduced performance.

4.2.5 After initiation, mission time-critical operations shall *not* require "ground-in-the-loop" commanding to enable successful operation/completion.

4.2.6 The launch sequence and other mission critical sequences shall 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.

4.2.7 Completion of the launch sequence shall leave the spacecraft/payload/instrument in a ground-commandable, safe state requiring no "immediate" time-critical ground commanding to assure health/safety.

4.2.8 Flight sequences to be used within the first 30 days after launch (e.g., contamination cover openings, trajectory correction maneuver) shall be test-verified on the spacecraft prior to launch.

4.2.9 Flight software loads/updates and sequence memory loads, particularly for those affecting mission critical capability, shall be verified by a memory readout or checksum readout. Depending on the application and mission/system consequence, single or multiple readouts shall be considered.

4.3 First Time In-flight Events

First time in-flight use of functionality, particularly for mission critical or irreversible events, shall receive special development attention (e.g., analyzing what-ifs, reviewing NFR's, identifying need for additional testing, identifying need for contingency plans) during the sequence development process to assure safe, reliable flight operation.

4.4 System Test Bed – Spacecraft/Payload/Instrument Fidelity

After launch, the ground system test-bed configuration/state shall be maintained as close as practical to the flight spacecraft/payload/instrument state - particularly the flight software code, parameters, counters, etc. - to minimize test initialization and run times and to provide high confidence in the test bed results.

4.5 Contingency Plans

4.5.1 For at least mission critical and first time in-flight events, contingency plans shall be developed to minimize the threat to health/safety of the mission in case of unexpected/improper spacecraft/payload/instrument response.

4.5.2 All contingency commands shall be system test-bed-verified prior to transmission to the spacecraft/payload/instrument. Additionally, launch related contingency plans should be test-verified on the spacecraft/payload/instrument.

4.6 Operating Margins

Adequate operating margins (e.g., memory, timing, power) shall be maintained for all stored sequence controlled and real-time flight activities to maximize the prospects for safe, reliable operation.

4.7 Telemetry Predicts and Alarm Limits

Subsystem telemetry measurement predictions and alarm limits shall 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.

4.8 Maintaining Health/Safety

Spacecraft/payload/instrument operations shall be consistent with maintaining health/safety. Hence, unnecessary risk-taking shall be avoided. If health/safety flight rule waivers are necessary to implement activities, the project manager shall approve waivers.

4.9 Fault Protection (F/P) Value Limit Strategy

Spacecraft/Payload/Instrument Autonomous fault protection enable/ disable strategy, threshold trigger values, and persistence values shall be established considering mission phase applicability and operational activity. The enable/disable, trigger, and persistence values shall be selected to ensure safety but not "hair triggered" to cause inadvertent F/P entry/execution.

4.10 Characterization and Evaluation

The flight operations team shall 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.

4.11 Power Cycling and Prime/Redundant Hardware Usage

4.11.1 Power cycling of mission-critical hardware shall be avoided.

4.11.2 Prime selected hardware elements shall remain in use for all operations.

4.11.3 Swapping to redundant hardware elements shall be limited to fault recovery actions to assure health/safety.

4.11.4 Simultaneous use of selected prime and redundant hardware to enhance reliability/performance for accomplishing mission critical activities shall be considered only after careful study, and shall be approved at the Flight Readiness Review.

4.12 Redundant Ground Coverage

Redundant ground coverage (e.g., site or antenna at same site) shall be planned during mission critical operations to guarantee real-time performance visibility and enable ground contingency commanding, if necessary.

5. Acronyms

AIT	Assembly, Integration, & Test
AO	Announcement of Opportunity
ASIC	Application-specific integrated circuit
BER	Bit error rate
CBE	Current best estimate
CCSDS	Consultant Committee for Space Data Systems
CDR	Critical Design Review
CM	Configuration Management
CM	Configuration Management
COTS	Commercial Off-The-Shelf
CP	Center Procedure
CPMC	Center Program Management Council
EDAC	Error Detection and Correction
EDL	Entry, Descent, and Landing
EM	Engineering model
EMI	Electromagnetic Interference
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
ESD	Electrostatic discharge
ESD	Electrostatic discharge
FMEA	Failure Mode Effects Analysis
FMECA	Failure Modes & Criticality Analysis
FPGA	Field-programmable Gate Array
FR	Radio frequency
FRR	Flight Readiness Review
GSE	Ground Support Equipment
H/W	Hardware
IR	Infrared
IV&V	Independent Verification and Validation
LMS	Langley Management System

MA	Mission Assurance
MDVT	Mission Design & Verification Test
NFR	Non-conformance Failure Report
PDR	Preliminary Design Review
POR	Power-on reset
PR	Procurement Requisition
PROM	Programmable Read-Only Memory
QA	Quality Assurance
RFP	Request for Proposal
RHU	Radioisotope Heater Unit
RSS	Root Sum Squared
RTG	Radioisotope Thermoelectric Generator
S&MA	Safety and Mission Assurance
S/W	Software
SAR	Systems Acceptance Review
SRR	Systems Requirements Review
TRL	Technology Readiness Level
UV	Ultraviolet

Guideline

Appendix: Software Principles for Flight Systems

Table of Contents

1 Introduction

Tighter development budgets and schedules, plus the proliferation of software throughout systems has made it mandatory to define, design, and implement flight software in a more disciplined manner. Process oversights are the root cause of many recent mission failures. Moreover, inadequate planning and ineffective implementation are common contributors to cost and schedule overruns. These software development principles emphasize the requisites of repeatable software processes in the Systems Engineering Competency.

Mission success (including personnel and equipment safety) is of paramount importance; risk, cost, and schedule are managed accordingly. Although applicable to other domains, mission-critical software is the primary target of the software development principles contained in this document.

Mission-critical software is identified by each project and typically includes flight software as well as software used in the integration and testing, uplink, downlink, and navigation processes. In addition to software, these principles also apply to the development of mission-critical firmware, through completion of testing in a simulated hardware environment. “Software development,” as used here, applies to both pre-delivery and post-delivery development activity; the latter is often called “maintenance.” The principles are intended to foster the needed discipline by documenting objectives within the organization. They elaborate the broader principles contained in this document and at the same time provide additional guidance on implementing the process requirements documented in the industry software standard; IEEE/EIA 12207.0.

In this initial version, the principles come from literature on software engineering and management (see Published Sources).

Software development — both in-house development and subcontracted/partnered development — should comply with each applicable principle through the deliberate and disciplined application of IEEE/EIA 12270.0.

1.1 Definitions

Acquirer: An organization that acquires or procures a system, software product, or software service from a supplier.

Note: The acquirer could be one of the following: buyer, ***customer****, owner, user, or purchaser.*

Acquisition: The process of obtaining a system, software product, or software service.

Contract: A binding agreement between two parties, especially enforceable by law, or a similar internal agreement wholly within an organization for the supply of software service or for the supply, development, production, operation, or maintenance of a software product.

Customer: The recipient of a product provided by a suppler. In the contractual situation, the customer is called the Acquirer. The Customer may be the ultimate consumer, user, beneficiary, or purchaser. The Customer can be external or internal to the organization.

Developer: An organization that performs development activities (including requirements analysis, design, testing through acceptance) during the software life cycle process.

Life cycle model: A framework containing the processes, activities, and tasks involved in the development, operation, and maintenance of a software product spanning the life of the system from the definition of its requirements to the termination of its use.

Maintainer: An organization that performs maintenance activities.

Operator: An organization that operates the system.

Supplier: An organization that enters into a contract with the acquirer for the supply of a system, software product, or software service under the terms of the contract.

Note:

1. *The term "supplier" is synonymous with contractor, producer, seller, or vendor.*
2. *The acquirer may designate a part of its organization as supplier.*

System: An integrated composite that consists of one or more of the processes, hardware, software, facilities, and people that provides a capability to satisfy a stated need or objective.

User: An individual or organization that uses the operational system to perform a specific function.

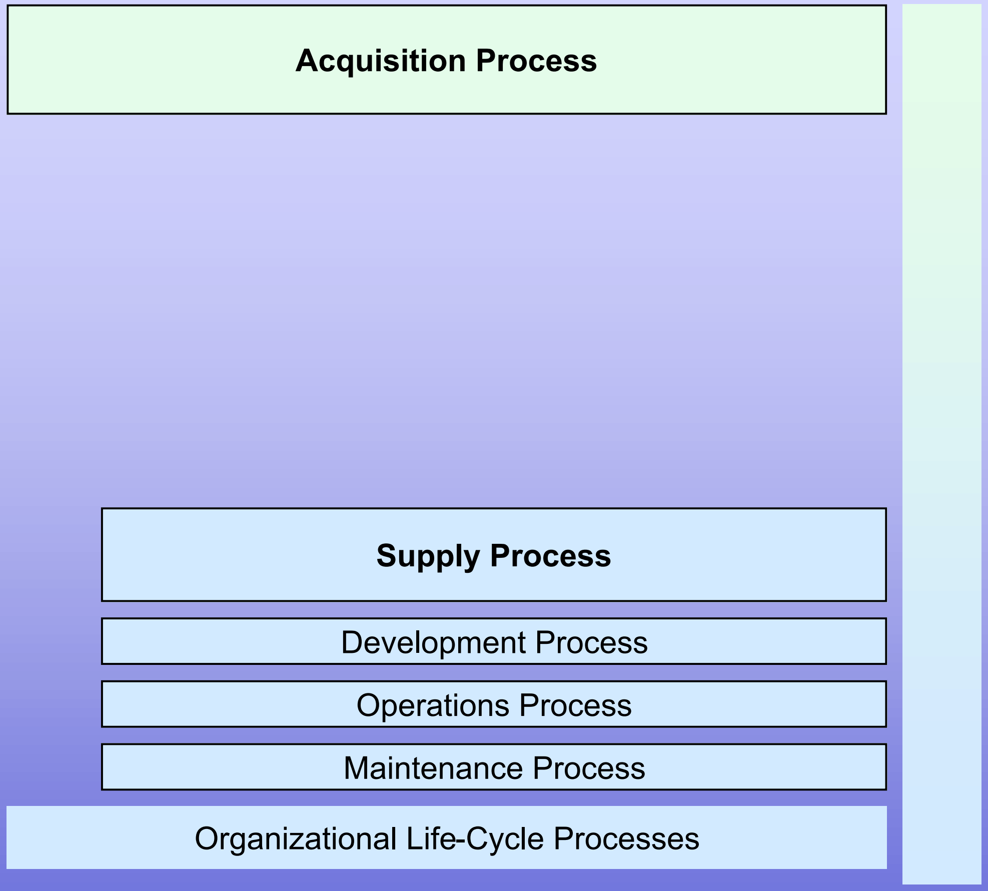
Note: *The user may perform other roles such as acquirer, developer, or maintainer.*

1.2 Overview

The general software principles presented in this guide are intentionally organized around life cycle processes to provide a foundation for the understanding and structured implementation of IEEE/EIA 12207.0.

The following figure gives a representative interrelationship between the sections (life cycle processes) of this appendix.

Process Overview



Acquisition Process

Supply Process

Development Process

Operations Process

Maintenance Process

Organizational Life-Cycle Processes

2 Primary Life Cycle Processes

The primary processes consist of five processes that serve primary parties during the life cycle of software. A primary party is one that initiates or performs the development, operation, or maintenance of software products. These primary parties are the acquirer, the supplier, the developer, the operator, and the maintainer of software products.

2.1 Acquisition Process

Defines the activities of the acquirer, the organization that acquires a system, software product or software service. The use of the acquisition process should achieve the following objectives:

a) Develop a contract, including tailoring of the standard, that clearly expresses the expectation, responsibilities, and liabilities of both the acquirer and the supplier;

b) Obtain products and/or services that satisfy the customer need;

c) Manage the acquisition so that specified constraints (e.g., cost, schedule, and quality) and goals (e.g., degree of software reuse) are met;

d) Establish a statement of work to be performed under contract;

e) Qualify potential suppliers through an assessment of their capability to perform the required software;

f) Select qualified suppliers to perform defined portions of the contract;

g) Establish and manage commitments to and from the supplier;

h) Regularly exchange progress information with the supplier;

i) Assess compliance of the supplier against the agreed upon plans, standards, and procedures;

j) Assess the quality of the suppliers delivered products and services;

k) Establish and execute acceptance strategy and conditions (criteria) for the software product or service being acquired;

l) Establish a means by which the acquirer will assume responsibility for the acquired software product or service.

2.2 Supply Process

Defines the activities of the supplier, the organization that provides the system, software product or software service to the acquirer. The use of the Supply process should achieve the following objectives:

a) Establish clear and ongoing communication with the customer;

b) Define documented and agreed customer requirements with managed changes;

c) Establish a mechanism for ongoing monitoring of customer needs;

d) Establish a mechanism for ensuring that customers can easily determine the status and disposition of their requests;

e) Determine requirements for replication, distribution, installation, and testing of the system containing software or stand-alone software product;

f) Package the system containing software or the stand-alone software product in a way that facilitates its efficient and effective replication, distribution, installation, testing, and operation;

g) Deliver a quality system containing software or stand-alone software product to the customer, as defined by the requirements, and install in accordance with the identified requirements.

2.3 Development Process

Defines the activities of the developer, the organization that defines and develops the software product. The use of the development process should achieve the following objectives:

a) Develop requirements of the system that match the customer's stated and implied needs;

b) Propose an effective solution that identifies the main elements of the system;

c) Allocate the defined requirements to each of those main elements;

d) Develop a system release strategy;

e) Communicate the requirements, proposed solution, and their relationships to all affected parties;

f) Define the requirements allocated to software components of the system and their interfaces to match the customer's stated and implied needs;

g) Develop software requirements that are analyzed, correct, and testable;

h) Understand the impact of software requirements on the operating environment;

i) Develop a software release strategy;

j) Approve and update the software requirements as needed;

k) Communicate the software requirements to all affected parties;

l) Develop an architectural design;

m) Define internal and external interfaces of each software component;

n) Establish traceability between system requirements and design and software requirements, between software requirements and software design, and between software requirements and tests;

o) Define verification criteria for all software units against the software requirements;

p) Produce software units defined by the design;

q) Accomplish verification of the software units against the design;

r) Develop an integration strategy for software units consistent with the release strategy;

s) Develop acceptance criteria for software unit aggregates that verify compliance with the software requirements allocated to the units;

t) Verify software aggregates using the defined acceptance criteria;

u) Verify integrated software using the defined acceptance criteria;

v) Record the results of the software tests;

w) Develop a regression strategy for retesting aggregates, or the integrated software, should a change in components be made;

x) Develop an integration plan to build system unit aggregates according to the release strategy;

y) Define acceptance criteria for each aggregate to verify compliance with the system requirements allocated to the units;

z) Verify system aggregates using the defined acceptance criteria;

aa) Construct an integrated system demonstrating compliance with the system requirements (functional, nonfunctional, operations, and maintenance);

bb) Record the results of the system tests;

cc) Develop a regression strategy for retesting aggregates or the integrated system should a change in components be made;

dd) Identify transition concerns, such as availability or work products, availability of system resources to resolve problems and adequately test before fielding corrections, maintainability, and assessment of transitioned work products.

2.4 Operations Process

Defines the activities of the operator, the organization that provides the service of operating a computer system in its live environment for its users. The use of the Operation process should achieve the following objectives:

a) Identify and mitigate operational risks for the software introduction and operation;

b) Operate the software in its intended environment according to documented procedures;

c) Provide operational support by resolving operational problems and handling user inquires and requests;

d) Provide assurance that software (and host system) capacities are adequate to meet user needs.

e) Identify customer support service needs on an ongoing basis;

f) Assess customer satisfaction with both the support services being provided and the product itself on an ongoing basis;

g) Deliver needed customer services.

2.5 Maintenance Process

Defines the activities of the maintainer, the organization that provides the service of maintaining the software product; that is, managing modifications to the software product to keep it current and in operational fitness. This process includes the migration and retirement of the software product. The use of the maintenance process should achieve the following objectives:

a) Define the impact of organization, operations, and interfaces on the existing system in operation;

b) Identify and update appropriate life cycle data;

c) Develop modified system components with associated documentation and tests that demonstrate that the system requirements are not compromised;

d) Migrate system and software upgrades to the user's environment;

e) Ensure fielding of new systems or versions does not adversely affect ongoing operations;

f) Maintain the capability to resume processing with prior versions.

3 Supporting life-cycle processes

The supporting life cycle processes consist of eight processes. A supporting process supports another process as an integral part with a distinct purpose and contributes to the success and quality of the software project. A supporting process is employed and executed, as needed, by another process.

3.1 Documentation Process

Defines the activities for recording the information produced by a life cycle process. The use of the documentation process should achieve the following objectives:

a) Identify all documents to be produced by the process or project;

b) Specify the content and purpose of all documents and plan and schedule their production;

c) Identify the standards to be applied for development of documents;

d) Develop and publish all documents in accordance with identified standards and in accordance with nominated plans;

e) Maintain all documents in accordance with specified criteria.

3.2 Configuration Management Process

The use of the Configuration Management process should achieve the following objectives:

a) Identify, define, and control all relevant items of the project;

b) Control modifications of the items;

c) Record and report the status of items and modification requests;

d) Ensure the completeness of the items;

e) Control storage, handling, release, and delivery of the items.

3.3 Quality Assurance Process

Defines the activities for objectively assuring that the software products and processes are in conformance with their specified requirements and adhere to their established plans. Joint reviews, audits, verification, and validation may be used as techniques of Quality Assurance. The use of the Quality Assurance process should achieve the following objectives:

a) Identify, plan, and schedule quality assurance activities for the process or product;

b) Identify quality standards, methodologies, procedures, and tools for performing quality assurance activities and tailor to the project;

c) Identify resources and responsibilities for the performance of quality assurance activities;

d) Establish and guarantee the independence of those responsible for performing quality assurance activities;

e) Perform the identified quality assurance activities in line with the relevant plans, procedures, and schedules;

f) Apply organizational quality management systems to the project.

3.4 Verification Process

Defines the activities (for the acquirer, the supplier, or an independent party) for verifying the software products and services in varying depth depending on the software project. The use of the verification process should achieve the following objectives:

a) Identify criteria for verification of all required work products;

b) Perform requirements verification activities;

c) Find and remove defects from products produced by the project.

3.5 Validation Process

Defines the activities (for the acquirer, the supplier, or an independent party) for validating the software products of the software project. The use of the validation process should achieve the following objectives:

a) Identify criteria for validation of all required work products;

b) Perform required validation activities;

c) Provide evidence that the work products, as developed, are suitable for their intended use.

3.6 Joint Review Process

Defines the activities for evaluating the status and products of an activity. This process may be employed by any two parties, where one party (reviewing party) reviews another party (reviewed party) in a joint forum. The use of the Joint Review process should achieve the following objectives:

a) Evaluate the status and products of an activity of a process through joint review activities between the parties to a contract;

b) Establish mechanisms to ensure that action items raised are recorded for action.

3.7 Audit Process

Defines the activities for determining compliance with the requirements, plans, and contract. This process may be employed by any two parties, where one party (auditing party) audits the software products or activities of another party (audited party). The use of the audit process should achieve the following objectives:

a) Determine compliance with requirements, plans, and contract, as appropriate;

b) Arrange the conduct of audits of work products or process performance by a qualified independent party, as specified in the plans;

c) Conduct follow-up audits to assess corrective action(s), closure, and root cause actions.

3.8 Problem Resolution Process

Defines a process for analyzing and removing the problems (including non-conformances), whatever their nature or source that are discovered during the execution of development, operation, maintenance, or other processes. The use of the problem resolution process should achieve the following objectives:

a) Provide a timely, responsive, and documented means to ensure that all discovered problems are analyzed and resolved;

b) Provide a mechanism for recognizing and acting on trends in problems identified.

4 Organizational Life-Cycle Processes

The organizational life cycle processes consist of four processes. They are employed by an organization to establish and implement an underlying structure made up of associated life cycle processes and personnel and continuously improve the structure and processes. They are typically employed outside the realm of specific projects and contracts; however, lessons from such projects and contracts contribute to the improvement of the organization.

4.1 Management Process

Defines the basic activities of the management, including project management, related to the execution of a life cycle process. The use of the management process should achieve the following objectives:

a) Define the scope of the work for the project;

b) Identify, size, estimate, plan, track, and measure the tasks and resources necessary to complete the work;

c) Identify and manage interfaces between elements in the project and with other projects and organizational units;

d) Take corrective action when project targets are not achieved;

e) Establish quality goals, based on the customer's quality requirements for various checkpoints within the project's software life cycle;

f) Establish product performance (memory, processing, communications) goals, based on the customer's requirements for various checkpoints within the project's software life cycle;

g) Define and use metrics that measure the results of project activities or tasks, at checkpoints within the project's life cycle, to assess whether the technical, quality, and product performance goals have been achieved;

h) Establish criteria, metrics, and procedures for identifying software engineering practices and integrate improved practices into the appropriate software life cycle processes and methods;

i) Perform the identified quality activities and confirm their performance;

j) Take corrective action when technical, quality, and product performance goals are not achieved;

k) Determine the scope of risk management to be performed for the project;

l) Identify risks to the project as they develop;

m) Analyze risks and determine the priority in which to apply resources to mitigate those risks;

n) Define, implement, and assess appropriate risk mitigation strategies;

o) Define, apply, and assess risk metrics to measure the change in the risk state and the progress of the mitigation activities;

p) Establish an environment that supports effective interaction between individuals and groups;

q) Take corrective action when expected progress is not achieved.

4.2 Infrastructure Process

Defines the basic activities for establishing the underlying structure of a life cycle process. The use of the infrastructure process should achieve the following objectives:

a) Establish and maintain a well-defined software engineering environment, consistent with and supportive of the set of standard processes and organizational methods and techniques;

b) Tailor the software engineering environment to the needs of the project and the project team;

c) Develop a software engineering environment that supports project team members regardless of the performance location of process activities;

d) Implement a defined and deployed strategy for reuse.

4.3 Improvement Process

Defines the basic activities that an organization (that is, acquirer, supplier, developer, operator, maintainer, or the manager of another process) performs for establishing, measuring, controlling, and improving its life cycle process. The use of the improvement process should achieve the following objectives:

a) Establish a well-defined and maintained standard set of processes, along with a description of the applicability of each process;

b) Identify the detailed tasks, activities, and associated work products for each standard process, together with expected criteria;

c) Establish a deployed specific process for each project tailored from the standard process in accordance with the needs of the project;

d) Establish and maintain information and data related to the use of the standard process for specific projects;

e) Understand the relative strengths and weaknesses of the organizations standard software processes;

f) Make changes to standard and defined processes in a controlled way;

g) Implement planned and monitored software process improvement activities in a coordinated manner across the organization.

Refer to Langley Management System for Improvement Process.

4.4 Training Process

Defines the activities for providing adequately trained personnel. The use of the Training process should achieve the following objectives:

a) Identify the roles and skills required for the operations of the organization and the project;

b) Establish formal procedures by which talent is recruited, selected, and transitioned into assignments in the organization;

c) Design and conduct training to ensure that all individuals have the skills required to perform their assignments;

d) Identify and recruit or train, as appropriate, individuals with the required skills and competencies to perform the organizational and project roles;

e) Establish a work force with the skills to share information and coordinate their activities efficiently;

f) Define objective criteria against which unit and individual training performance can be measured, to provide performance feedback, and to enhance performance continuously;

Refer to Langley Management System for Training Process.

5 Published Sources

Information in this appendix is taken from the following:

1. IEEE/Electronic Industries Association (EIA) 12207.0-1996, IEEE/EIA Standard, Industry Implementation of International Standard International Organization for Standardization (ISO)/International Electro-technical Commission (IEC) 12207: 1995, Standard for Information Technology – Software Life Cycle Processes.
2. IEEE/EIA 12207.1-1997, IEEE/EIA Standard, Industry Implementation of International Standard ISO/IEC 12207: 1995, Standard for Information Technology – Software Life Cycle Processes – Life Cycle Data.

6 NASA Software Policy

NASA policy guidance for SEC Flight Software Projects:

1. NASA Policy Directive 7120.5, NASA Program and Project Management
2. NASA Policy Directive 2820.1, NASA Software Policies

3. NASA Policy Directive 8730.4, NASA Software Independent Verification and Validation (IV&V) Policy