Safety and Mission Assurance

Risk-based Prioritization Handbook for Space Flight Projects

NASA
Goddard Space Flight Center

April 2020

National Aeronautics and Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

SIGNATURE PAGE

Prepared by: JESSE LEITNER Digitally signed by JESSE LEITNER Date: 2020.06.10 14:10:22 -05'00' Date: 6/10/20

Jesse Leitner
Chief Engineer, Safety and Mission Assurance

Reviewed by: Digitally signed by DAVID PETRICK DN: c=US, o=U.S. Government, ou=NASA, ou=People, cn=DAVID PETRICK, 0.9.2342.19200300.100.1.1=dpetrick Date: 2020.06.10 15:41:03 -04'00' Date: 6/10/20

Dave Petrick
Assistant Director/Technical, Safety
and Mission Assurance

Reviewed by: MICHAEL VIENS Digitally signed by MICHAEL VIENS Date: 2020.06.11 14:19:00 -04'00' Date: 6/11/20

Michael Viens
Chief Engineer, Quality and Reliability

Approved by: CATHERINE PEDDIE Digitally signed by CATHERINE PEDDIE Date: 2020.06.19 16:39:33 -04'00' Date: 6/19/20

Eric K. Isaac
Director, Safety and Mission Assurance

CHANGE HISTORY LOG

REV LEVEL	DESCRIPTION OF CHANGE (Note if Baseline, Change, Reissue)	APPROVED BY	DATE APPROVED
-	Baseline Issue	CCR-D-0133	06/19/2020

TABLE OF CONTENTS

SECTION PAGE

Table of Contents

1. SCOPE

1.1 Purpose

This handbook provides recommended guidelines for prioritizing mission success activities for highly constrained space flight projects, such as those Classified as D or below, per GPR 8705.4, or projects with lower tolerance for risk that are affected by significant constraints that limit the efforts performed for mission success. It is important to point out that this document is not intended as a prescriptive manuscript to describe every activity needed for mission success, but rather as a tool to promote critical thinking about how to select and structure activities for mission success, providing general assessments of the relative return on investment for common activities that support development and test.

1.2 Applicability

The guidance set forth in this document is targeted to support any project that has cost, schedule, or technical constraints that prevent the use of the broad engineering and SMA practices typically applied for mission success for GSFC missions. However, it may be applied to a project at any level of risk-tolerance that requires prioritization due to resource constraints.

This handbook may be cited in contracts, program, project, and other Agency documents to provide technical guidance.

2. APPLICABLE DOCUMENTS

2.1 General

Documents listed in this section contain provisions that constitute underlying guidance and requirements related to the implementation guidance provided in this handbook. In general, the latest issuances of the cited documents should be used. The applicable documents are accessible via the NASA Technical Standards System at http://standards.nasa.gov and the Goddard Directives Management System at https://gdms.gsfc.nasa.gov/GDMSv2/index.htm.

2.2 Government Documents

GSFC-HDBK-8007	Cubesat Mission Success Activities
GSFC-STD-7000	General Environmental Verification Standard
GPR 8705.4	Risk Classification and Risk-based Safety and Mission Assurance for GSFC Payloads and Systems

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

AC	Alternating Current
C	Celsius
CE	Conducted Emissions
CM	Configuration Management
CS	Conducted Susceptibility
DC	Direct Current
EEE	Electrical, Electronic, and Electromechanical
EGSE	Electrical Ground Support Equipment
EMI	Electromagnetic Interference
FMECA	Failure Modes Effects and Criticality Analysis
FOD	Foreign Object Debris
FPGA	Field Programmable Gate Array
FTE	Full-time Equivalent
GEVS	General Environmental Verification Standard
GMIP	Government Mandatory Inspection Point
GPR	Goddard Procedural Requirement
GSFC	Goddard Space Flight Center
HDI	High Density Interconnect
HiPot	High Potential
HV	High Voltage
I&T	Integration & Test
IPC	Association Connecting Electronics Industries

ISS	International Space Station
LxC	Likelihood and Consequence
MAR	Mission Assurance Requirements document
MIL-SPEC	Military Specification
MIUL	Materials Identification and Usage List
MoS	Margin of Safety
MUA	Materials Usage Agreement
OBE	Overcome by Events
PCB	Printed Circuit Board
PDR	Preliminary Design Review
PFR	Problem Failure Record
PSA	Parts Stress Analysis
RCCA	Root Cause and Corrective Action
RE	Radiated Emissions
RS	Radiated Susceptibility
SEMP	Systems Engineering Management Plan
SMA	Safety & Mission Assurance
STD	Standard
TA	Technical Authority
TVAC	Thermal Vacuum

3.2 Definitions

Highly-Constrained Project	A project, typically Class D or below, that does not have the resources (time or money) available to perform the full suite of activities generally performed on GSFC projects. Note that typically GSFC projects have extensive piece-parts screening and mandatory inspection efforts that can use significant resources. A highly-constrained project is much less likely to have the resources available if a similar approach is employed.
Issue or Problem	A risk that has been realized, whether or not the risk was known a prior.
Mission Success Activities	Activities that would typically be included in a mission assurance requirements document (MAR), an environmental test plan, systems engineering management plan (SEMP), or other similar document geared toward assuring success in meeting project objectives
Mission Success Plan	A collection of mission success activities into a cohesive plan that ultimately may be used a single document for a highly-constrained project (such as a "do no harm" classified project) that has minimal documentation requirements, or apportioned out into other documents, such as a MAR, a SEMP, or an environmental test plan.
Problem Failure Record	A problem that, upon analysis, is determined to entail significant risk to mission success or to otherwise necessitate a project-level review board for disposition.
Risk	The combination of 1) the likelihood (qualitative or quantitative) that a project, program, or organization will experience an undesired event such as cost overrun, schedule slippage, or failure to achieve a required outcome, and 2) the associated consequence or impact of the undesired event were it to occur.
Risk Assessment	The formulation of one or more statements of risk based on analysis of the supporting data associated with a concern.
Root Cause	1. The organizational factor that led to decisions made or processes employed 2. Cause below proximate and intermediate causes and there is no further "why" questioning that would be meaningful. 3. The flaw in the process or processes that enabled the failure.

4. GETTING STARTED

GSFC has a long history of successfully developing and operating large, complex space missions. Much of the success is a result of proven longstanding practices that ensure that no

stone is unturned to wring out defects and risky elements, and verify that the system is functioning as expected. Historically, the consideration for cost has centered entirely around the cost of an on-orbit failure and minimal emphasis has been placed on containing the costs of development. As the Agency continues to strive for doing more science and exploration with less resources, the concepts of Class D and sub-Class D missions become more prevalent. In order to carry this forward, it is necessary to employ assurance practices that are more focused on the actual risks for the mission, as the resources will not be available to provide all of the barriers of protection that have become traditional for our larger missions. Many of these barriers of protection, be they screening processes, detailed inspections, or other processes that involve strict government oversight and approvals of contractor work involve front-loaded investment, insertion of uncertain amounts of schedule, and potential reaction to nonconformances that may not entail risk. The effect of this is to tap into margins or the direct allocations for critical back-end activities, such as system-level testing, time to resolve problems (e.g. root cause and corrective actions for Problem Failure Records, or PFRs), and time to assess risks and capture lessons (some of the most important things to ensure that a system will function when it gets on orbit and that no matter what happens with the mission, the experience will be valuable). The guidance provided in this document is based on extensive GSFC experience and that of its contractors and subcontractors.

4.1 Working under limited resources

One of the big challenges that has arisen is that of how to allocate the appropriate assurance processes for a mission that is Class D or below, given the fact that there are not resources available to employ all of standard practices of high-end missions. Consequentially, we put forth in this document a priority set of assurance activities to aid in the process of selecting activities when resources are not available to perform all or most of them. While the scope of this document covers SMA activities, environmental testing elements are included for a holistic picture to promote thoughts about a more granular look at the overall development and testing campaign. Responsibility for ultimate selection of environmental test activities rests in Code 500, and is left to the Mission Systems Engineer (MSE). This is not meant to be a one-size-fits-all cookbook, but it is intended to provide general guidance as well as a sanity check to inform development of a Mission Assurance Requirements document (MAR) and to coordinate with an environmental test plan. Some items are so fundamental (e.g., resolve all problems and capture and manage risks) that there would be no reasonable determination that they should be excluded.

The items are collected into Groups, which subjectively provide comparable levels of risk buy down in exchange for resource and “risk investment”. The earlier Groups provide the most payoff in terms of risk reduction (the first Group being fundamental to apply to any mission), given the investment, while the later Groups tend to be costlier and buy down less risk for the given investment. In many cases, overindulgence on the items in Groups C-E on a highly-constrained project results in reduced ability to complete common-sense efforts that occur late in development and testing or reduced attention to activities that appear to be less tangible to the final product. The ordering of Groups is based on general measures of effectiveness in buying

down risk, not necessarily the direct costs of implementing the particular processes. In some sense it is ordered by how much technical risk is reduced for a given amount of cost and programmatic risk (risks of failure in I&T or of schedule lost by performing them), in short based on notional ratios of (1) technical risk reduced to resources used, and (2) technical risk reduced to programmatic risk incurred.

> Example:
> Thermal vacuum testing can be extremely costly, but the first two TVAC cycles can be especially effective in eliminating defects that would likely cause failures and anomalies when on-orbit. While TVAC testing may prompt some failures on the ground it is not likely to elevate risk, since the failures are most likely relevant. Thus, TVAC testing has a relatively low ratio of resources and programmatic risk to technical risk buydown, making it a good return on investment, particularly for the first two cycles or so. On the other hand, some forms of conduced susceptibility (CS) EMI testing are not excessively costly, but they are in some sense designed to make the hardware electrically "bullet-proof", and in doing so can prompt failures that are very unlikely to be encountered on-orbit. Likewise, piece-part-level screening puts the parts through extreme rigors, often at high costs, but they often prompt failures that would not happen under normal or even typical elevated operational conditions, and they may also put unreasonably stress on parts that are not overdesigned for the application, driving up risk and reducing lifetime. Thus, these two examples have a relatively high ratio of resources and programmatic risk to technical risk bought down. Note that while bolded items are the top candidates for restrictively using on all projects, they are not all at the top of Group A in order to help in the organization of the document.

4.2 Informing the selection of mission success activities

A key emphasis in this document is the consideration of the specific mission qualities, environment, and design attributes to inform the selection of mission success activities to perform, as an alternative approach to the use of longstanding, broad mission assurance and environmental test requirements that assume typical Class B mission constraints. The prioritization logic employs a "right-to-left" development approach: one that protects back-end problem-solving and system testing and evaluation activities while focusing the use of piece-part screening and qualification efforts only for select critical items that have a limited knowledge base. This contrasts the typical "left-to-right" development approach that puts significant resources into piece-part screening and qualification activities that limit back-end resources available for the processes that are most effective in making sure the system is going to work reliably on-orbit. For large missions, there are plenty of resources to make sure problem resolution and testing are complete, but not necessarily for overconstrained projects. In short, the right-to-left approach protects the resources for problem-solving and system-testing in a flight configuration, while being as selective and focused as possible to apply piece-part level screening activities to limited areas based on factors such as criticality, familiarity, and historical performance. This is illustrated in Figure 1 below

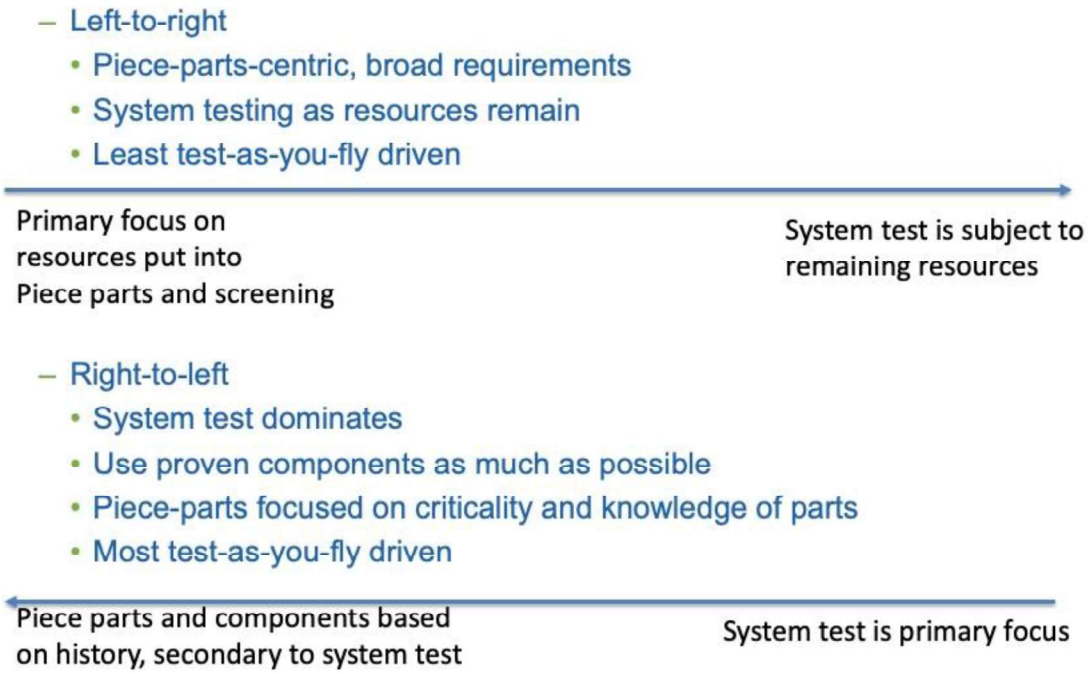

Figure 1. Left-to right vs right-to-left development comparison

It should be acknowledged here that the "right-to-left" approach is much more challenging but no more so than to successfully implement an over-constrained project. The left-to-right approach is more intuitive, with sequential planning, but it is success-oriented, so if significant delays and resource usage are caused by screening processes, either reduction of the most important activities (testing and problem resolution time) will occur, or an overrun or cancellation. Right-to-left development holds the most critical activities as sacred, while piece-parts activities are selectively driven based on risk.

4.3 General Procedure for building the mission success plan

Refer to Table 1, which includes activities bundled into 5 Groups, where the Groups constitute Returns on Investment (ROI) for risk buydown, where Group A is the maximum ROI and Group E is the minimum within this framework. Figure 2 shows a flow diagram, with expanded detail below:

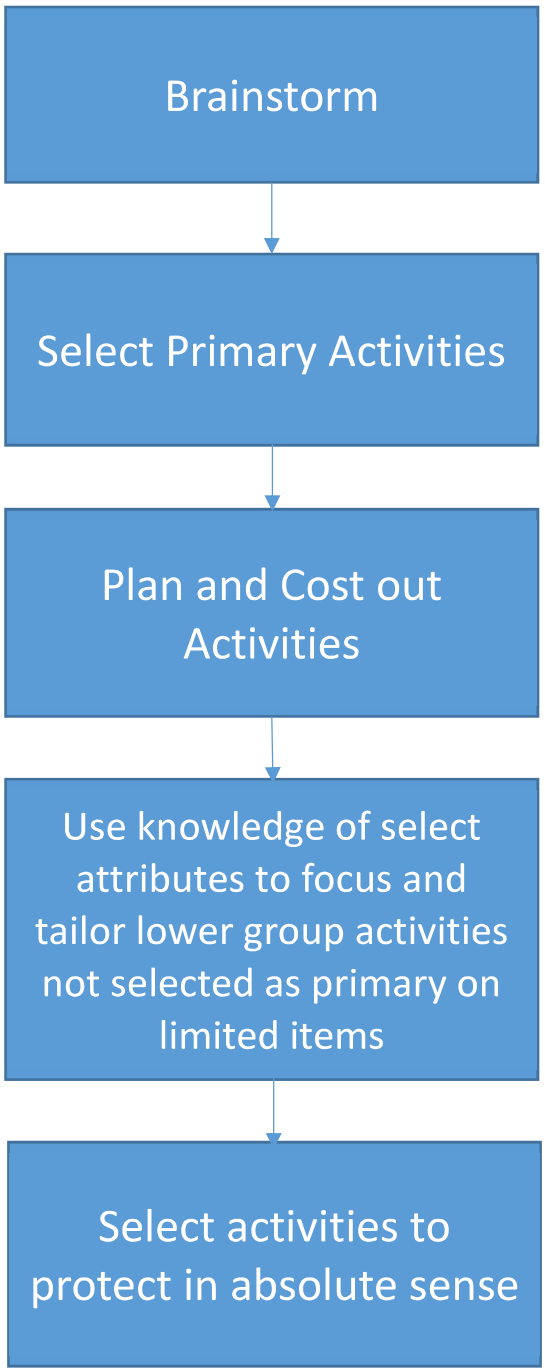

Figure 2. Activity Selection Flow Diagram

Step 1: Brainstorm mission attributes, such as number of spacecraft, cubesat vs smallsat vs instrument, inherent fault-tolerance/redundancy, heritage of the design, use of high voltage, known sensitivities of components, etc. This will become the springboard from which to select

activities. If upfront reliability and risk assessment is performed, the results should help inform this effort.

Step 2: Select items from Groups, working down from Group A, factoring in specific mission attributes to adjust as needed (e.g., multiple spacecraft, orbital regime, inherent fault tolerance of the design, build-to-print of previous spacecraft and/or instruments, etc.) There may be some elements of this list that would demand some reordering based on the particular mission attributes, particularly after Group A. In some cases, sine vibe may be a more effective first line of defense than random vibe.[1] Likewise, since vacuum testing can be extremely costly, for some missions ambient thermal cycling, at least for most thermal cycle testing, may flush out most of the related problems when (1) there are limited vacuum-sensitive components, (2) printed circuit boards are not particularly complex or sensitive designs, and (3) expectations for moisture-driven failure scenarios are limited. The ultimate decision is the responsibility of the MSE with subject matter experts in Codes 540 and 560 and outside of the scope of this guidance. Activities to prevent harm to a host platform or to ensure safety of personnel and the public (mandatory) should be established prior to those that assure mission success. These include host interface protection requirements (e.g., fusing, contamination protection, etc), ISS safety requirements as applicable, etc. It is essential to understand requirements and expectations of the host before moving into building the collective plan of activities.

Step 3: Plan and cost out all activities from highest priority to lowest.

Step 4: Use knowledge of critical aspects of the system, or those with less prior experience or associated with less experienced or less capable vendors to identify select items from the lower Groups to apply to certain specific parts or printed circuit boards.

Step 5: Choose processes to protect in an absolute sense – many recommended in bold below.

When using this document to evaluate an overall approach to SMA for a project, look for activities that are far out of place, e.g., those from far down the list that are broadly (as opposed to being applied to a few select items) implemented when many above are not implemented. This suggests that the selection of a limited set of activities may not be based on the proper considerations.

4.4 Revisiting based on experiences

The plan should be revisited based on experiences and issues that appear during development and should as a standard practice be reviewed at check points during and at the culmination of Mission Phases B and C. In particular, always be prepared to descope items (primarily in groups

[1] See GSFC-STD-7000, General Environmental Verification Standard (GEVS) for rationale associated with various classes and levels of environmental test. Note that GEVS testing levels and complete testing suites are very conservative, tuned primarily for Class A and B missions. GSFC-HDBK-8007, CubeSat Mission Success Handbook includes a version of GEVS tuned to CubeSats and highly-constrained smallsats.

C-E) based on observed limited effectiveness, those that are overcome by events (e.g., analyses that have not been completed in time for them to be effective), and those that will diminish critical back-end activities such as system-level testing and problem resolution.

Table 1. Ordered priorities for mission success

Group A	
Implement safety-first culture[2]	Safety may not be compromised under any circumstances.
Secure the ability to learn from any failures that occur (extra protection for communication or tracking ability, data recording and retrieval, etc)	The number one objective from flying small, low cost, high risk missions is to enable innovation and learn better, more efficient, and more effective processes to employed on all missions. This may result in, e.g., use of only proven products for data storage and communication, added fault-tolerance, etc.
Complete system testing with margin for sufficient hours in relevant environment[3]	If system test campaign has been completed successfully to cover the full environment (including launch) plus margin, and system functions prior to launch, then it is most likely to function upon orbit insertion.
First two TVAC cycles	Primary means to wring out defects, particularly those related to moisture, vacuum sensitivity, and printed circuit board internal flaws. Vacuum may be skipped for projects under extreme constraints that do not have vacuum sensitive components or the potential for moisture driven effects. The first hundred hours in vacuum is very effective for exposing flaws in printed circuit boards and moisture-sensitive parts that are not apparent in coupons, as moisture buried internally to such components is evacuated, tending to pass through undesired conductive paths, resulting in short or resistance-loss conditions.
First four T cycles (would include any in vacuum)	Wring out temperature sensitive components and workmanship flaws.
200 testing hours, last 60 failure-free per year of required operation	Primary means to establish system-level reliability

[2] Bolded items should apply to all projects as a top priority

[3] Highlighted items represent engineering responsibility only potentially influenced by SMA. Included here to ensure a complete picture of interacting and potentially competing elements under significant constraints.

Random vibe (sine vibe)	Workmanship and launch survival verification
EMI self-compatibility	Flesh out any internal electronic interference within components, instruments, and other subsystems. Important for any system with EMI-sensitive components and components that emit EM energy.
Radiation-tolerant design	Understand the radiation environment, and acknowledge imminent radiation effects. Ensure that the design is resilient to the radiation effects present in the area, be they single event or cumulative. Use a mix of redundancy, hardness/shielding in limited cases, and other means of fault tolerance. Applies to any project in a radiation environment
Strict Test Like You Fly practices	Going outside of "test like you fly" will risk either encountering untested conditions or performing overly conservative tests that may result in a failure that is not relevant (making it more likely for cancellation).
Resolve all problems or bound the risk (implement RCCA)	If testing covered the full environment then the primary risks that remain would be due to unresolved problems or taking parts or components close to or above rated limits.
Capture and manage risks rigorously	Without doing so will lead to poor decisions under limited resources resulting in inefficient development processes or on-orbit failures
Senior mentor involvement at .05-0.1 FTE (typically systems engineer or seasoned SMA invidual with strong discipline experience developing flight hardware)	While appropriate to outfit a high-risk-posture mission with new personnel with new ideas, senior mentoring is essential to make sure that the myriad of things that cause problems in missions that are not written down are prevented or caught early. Implement if at all possible.
Engineering Analysis	
Quick worst case circuit analysis on interface compatibility	Will electronics become overstressed in certain extreme conditions or operational scenarios, or after some period of time. Especially should employ on new designs that are pushing high performance/throughput.

Derate parts and components, part stress analysis	Most important activity to ensure reliability of parts. Any mission that has an extended lifetime should pay close attention to derating.
Strength analysis/testing, MoS	Ensure survival in testing and subsequent launch. Likely will be required by host or launch opportunity.
Maintain margins on components with limited/insufficient success history	Whether it be number of cycles, mass, volume (immature designs), operating power levels, etc.
Peer engineering design reviews	No matter how good a designer you have, he or she will always miss some things
Cell phone photography of all stages of development	Great and convenient way to document all work performed
Upfront Management System Quality Engineer (MSQE) process review.	Helps insure the process controls are defined and applied upfront to reduce risks and resources spent to correct issues later.
Upfront risk, reliability and criticality assessment	Helps determine critical areas to focus limited resources and other areas that require less attention. Formality may vary.
Use trained workmanship techs that have successful NASA experience	It can be very costly to demand and verify strict adherence to workmanship requirements, but using people who are experienced at NASA workmanship will likely result in products that meet requirements, particularly in areas that entail significant risk
ESD Training	All people handing space flight hardware should have had formal ESD training at some point. For out of house work, developer ESD training is sufficient. Formal certification generally need not be required for projects with some elevated tolerance for risk.
M&P Engineer Design and Drawing Review for New Designs	Having a NASA or developer M&P Engineer review new designs and drawings is the most cost-effective way to avoid M&P related issues during manufacturing, assembly, and test. Since the performance and interactions of materials and processes can have system-level impacts (e.g. outgassing), it is important to have the same M&P engineering organization

	review *both* the overall design of assemblies and the detailed design of individual parts. Note: by their very nature, materials and processes related problems discovered at the system level are *extremely* difficult to fix.

Group B	
IPC 6012 Class 3 for PCB specification with flexibility	Use class 3 as a target but strict interpretation may lead to unnecessary use of resources and elevated risk. Flexibility is particularly important if the boards have high density of parts or parts have very tight pin pitch, such as with high-density SRAMs or reconfiguration FPGAs (e.g., RTG4, Virtex-5 or later, Proasic-3, etc)
Design for manufacturability	Especially for new components, a short development duration project can drain all of its time and resources trying to manufacture a product that is overly sensitive to workmanship variations or other similar factors.
Radiation testing to inform risk as necessary.	To fill gaps or reduce some areas of redundancy or other forms of conservatism in the radiation tolerant design process. Especially for a constrained project, this should not supplant good radiation-tolerant design practices.
Use familiar parts to the greatest extent	Unfamiliar parts may bring significant uncertainty to your reliability. This may not always be an option.
Test all components and unfamiliar parts in relevant environment with margin	Helps avoid any surprises at system level
Vendor printed circuit board coupon analysis	Helps to buy down some programmatic risk of an inconvenient failure in I&T. Most important for a critical circuit being built by a bare board manufacturer not experienced in building successful space products.
Closeout inspection, inspection of high-risk elements with inexperienced developers or	Before buttoning things up, after which it may be very risky to get back in, make sure all is installed properly with no problematic

limited product history (well placed GMIPs during build cycle)	features (FOD, tight bend radii, etc). Not likely possible for most COTS assemblies.

Group C	
Two more TVAC cycles (in addition to first two, may be covered if first four thermal cycles are in vacuum)	Catch any lingering problems not caught earlier. This can be fairly costly unless a belljar is available that supports the hardware.
Independent PCB coupon testing	Mainly confine to new designs and particularly sensitive or critical components, or those with unfamiliar vendors
Reliability analysis (FMECA and/or fault-tree) completed at least 6 months before PDR to enable fault-tolerant design	Early timing can provide top areas to key in on for adding fault tolerance. Emphasis should be for new, complex designs.
Use of engineering models for high risk or unfamiliar components and subsystems	Good way to buy down risk when there is uncertainty in how the design will perform
FPGA peer review	A must for new complex and critical FPGA designs
Self-performed software assurance	Particularly for software-intense projects
Have a CM system, even if freeware (e.g.: SVN)	Helps avoid very big headaches
Bug reporting system (e.g., Jira)	Helps avoid repeated problems
Workmanship Training	For in-house work, NASA/GSFC workmanship certification for NASA inspectors (when required). For operators, formal workmanship training at some point should be sufficient. For out-of-house work, developer workmanship requirements and training is generally sufficient as a priority activity.
M&P Plan, Outside Developer	A formal M&P plan provides insight into existing M&P practices at outside developers. Previously documented vendor practices should be accepted in the place of a formal project-specific M&P Plan whenever practical.

	When working with large and well established developers with a previous history at GSFC, M&P plans should be accepted via the Inherited Items Process whenever practical. A formal M&P plan can be extremely useful in cases where an outside developer has little to no experience working with GSFC.

Group D	
Internal alert disposition and counterfeit protection	Avoid common part, material, or process problems that have affected other projects
Follow J-STD for workmanship, select inspections	Follow uniform workmanship requirements and select critical boards
Part screening, level 3 or use of MIL-SPEC parts where applicable	Ensures that parts are representative of similar parts used in previous applications. MIL-SPEC parts also bring traceability, tighter controls, and wider operating ranges, when needed. Use of available MIL-SPEC parts or manufacturer high-reliabilty parts will help reduce infant mortality. Infant mortality with EEE parts is not as common as it was in the early 2000's and before.
CS and RS testing	Good way to make your system bulletproof against a broad array of realistic and improbable electrical disturbances. These tests can involve significant risk that may not be present on orbit, so when project is highly constrained, they should be focused on areas where there is high uncertainty of the EMI environment and particular sensivity expected.
Four more TVAC cycles	Capture further lingering problems not caught earlier
Material Usage Agreements	Ensure that MUA codes are being used on the MIUL to minimize the number of MUAs requiring formal NASA review and approval
Material Certifications for Critical Items	Protectioon needed for the critical items whose failure would lead to either personal injury or loss of life.

Group E	
Thorough worst-case analysis	Look for any possible opportunity for a part to become overstressed in the most extreme situations. Useful in cases where there is substantial uncertainty in the operational environment.
Prohibited materials risk assessment	Assess risk in all cases of use of pure tin, cadmium, etc. Mainly should be considered for new, unproven designs.
Level 2 part screening for non MIL-SPEC parts	Tighten the bounds on part uniformity for non-MIL-SPEC parts. Could become a huge cost driver with very little risk payoff, so should be confined to applications where many parts are not sufficiently derated due to project constraints such as availability on schedule..
IPC 6012DS	Enforce extremely tight specs on printed circuit boards. Will add significant challenge and resource usage if high-density components are used (HDI). Generally should restrict to designs that have already been successfully built to 6012DS.

There are many more items to consider for mission success that are even more dependent on the specific mission attributes. These include:

- Team dynamics, co-located teams, matched for mission classification, etc.
- Identification of Descopes
- Early interface testing
- Full regression testing on all software.
- Engineering model and sparing plan per GPR 8730.10 Appendix (none, parts kits, built spares, tested spares, card-level, unit level, etc.)
- Risk-based decision making – don't drag it out for weeks/months in most cases
- Signal Integrity – where necessary (need criteria, order of importance; critical nets, high speed, eye diagrams, S-Parameters, cross-talk, etc.)
- Power Integrity – where necessary (need criteria, order of importance; DC drop analysis, AC analysis, capacitor mounting, current density, etc.)
- Dry runs for major reviews (how much time do projects waste on "telling the right story")

- EEE long lead parts procurement (are the parts long lead due to screening or technology)?
- Thermal analysis
- Balance between vacuum and ambient thermal cycle testing
- Sound grounding architecture for flight system and EGSE test bed
- Safe-to-mates (everything to ground, every pin to every pin)
- HiPot testing
- Avoid after-the-fact, OBE (overcome by events) products and analyses. Be ready to cut losses on such items:
    - Reliability analyses after system design is frozen
    - Expending major efforts to close paperwork on engineering model work when the flight model is in mature development and has departed from and surpassed the engineering model (unsolved problems that are pertinent to the current flight model should be brought to completion or have risk bounded).

Effects of specialized scenarios:

1. 4 or more (N) spacecraft
    a. Distinguish between workmanship and design validation for testing and assurance methodologies
        i. EMI self-compatibility on all spacecraft
        ii. Limit to CE and RE testing for 2-N
        iii. Workmanship level vibe at acceptance levels for 2-N
        iv. 2 TVAC cycles on 2-N
    b. Reduce design related testing on S/C 2-N
    c. Perform constellation reliability assessment
        i. Look for opportunities for graceful degradation based on loss of functions on individual spacecraft
        ii. Always protect ability to meet debris requirements
    d. Consider further reductions to enable adding an N+1st spacecraft
2. Extended thermal environment. < -20 C or > 85 C
    a. Bump up part screening to Group A, preference for MIL-SPEC parts
3. High voltage (> 1 kV)
    a. GMIPs on cable developments for HV elements
    b. Extended HV (e.g., partial discharge) testing on HV parts
    c. Look carefully at prior part usage and compare to current voltage levels, switching levels, etc.
    d. Be as conservative as possible for derating HV parts and components.
4. Cryo applications
    a. Will be extremely challenging for a highly-resource constrained project, requiring a very specialized and selective SMA and environmental test program