MEASUREMENT SYSTEM IDENTIFICATION

NASA TECHNICAL STANDARD **National Aeronautics and Space Administration**	**NASA-STD-8729.1A**
	Approved: 2017-06-13 **Superseding NASA-STD-8729.1**

NASA RELIABILITY AND MAINTAINABILITY (R&M) STANDARD FOR SPACEFLIGHT AND SUPPORT SYSTEMS

DOCUMENT HISTORY LOG

Status	Document Revision	Approval Date	Description
Baseline		1998-12-01	Initial Release
Revision	A	2017-06-13	Hierarchy showing the top level concerns while systematically providing more specifics that a project will need to address to assure reliability is designed and built into systems.

FOREWORD

This NASA Standard describes a technical basis for promoting and implementing Reliability and Maintainability (R&M) concepts on all new NASA programs and projects. The R&M Standard is meant to establish and promote a high level of R&M managerial and technical excellence throughout NASA. This Standard provides a comprehensive set of objectives and strategies against which programs and projects can plan and evaluate activities that directly affect the R&M activities. The Standard *recommends* evidence (controls, analysis, testing or inspection) that R&M engineers, and other relevant technical disciplines, that impact reliability of spacecraft, can provide in the planning and execution of a program or project over the lifecycle. It is meant to be comprehensive, but not prescriptive, in its description of objectives and strategies affecting reliability of programs and projects in NASA. The Standard does not preclude bringing forth evidence that is part of the spectrum of assurance activities across other disciplines and that must occur over the life cycle.

In pursuing an objectives based approach, the Office of Safety and Mission Assurance (OSMA) has determined that its policies and requirements relevant to spaceflight, aeronautics, and other research programs and projects must be better aligned with the program and project management approach defined in NPR 7120.5, NASA Space Flight Program and Project Management Requirements. This R&M Standard has been developed in accordance with this approach. The vision in general is to move from a process-based approach to one that is more rooted in the technical objectives of the stakeholders and Centers and is aligned with systems engineering. In other words, this Standard promotes defining requirements with the focus of meeting the defined technical objectives.

Currently NASA uses the policy directive NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy as a statement of its policies regarding their Reliability and Maintainability Program. Additionally NASA Standard 8729.1, *Planning, Developing and Maintaining and Effective Reliability and Maintainability Program,* is used to provide guidance on the role of R&M. This new R&M Standard will replace 8729.1 and will be used as the basis for planning activities to assure reliability of NASA programs and projects.

This NASA-STD was developed by NASA Headquarters, OSMA. Requests for information, corrections, or additions to this standard should be submitted to the National Aeronautics and Space Administration, OSMA, by email to Agency-SMA-Policy-Feedback@mail.nasa.gov or via the "Email Feedback" link at https://standards.nasa.gov.

Terry Wilcutt

Terrence W. Wilcutt
Chief Safety and Mission Assurance

6/13/2017
Approval Date

TABLE OF CONTENTS

LIST OF APPENDICES

RELIABILITY AND MAINTAINABILITY STANDARD FOR SPACEFLIGHT AND SUPPORT SYSTEMS

1. SCOPE

1.1 Purpose

1.1.1 This document specifies technical objectives and related strategies for NASA programs and projects to be used in planning, executing and evaluating Reliability and Maintainability (R&M). These objectives include a comprehensive set of considerations for projects and programs utilized as specified that impact reliability, as well as the specific activities for the R&M technical discipline. These considerations relate to R&M during the design, evaluation, and operation of spaceflight systems, and establish guidelines for the planning and review of related engineering and assurance activities across the lifecycle. This set of objectives, strategies and implementation guidelines are intended to promote a high level technical excellence in achieving R&M goals for all programs and projects.

1.1.2 Mandatory elements of this Standard require programs and projects to use these objectives and strategies during the planning of activities and formulation of requirements, and establish and justify to what extent and in what way they are addressed, commensurate with the accepted level of risk to safety and mission success. Upon agreement by the stakeholders and Safety and Mission Assurance (SMA) Technical Authority, the program or project is required to act in accordance with their plan. The program is expected to demonstrate that the various objectives identified in the plan are satisfied to an acceptable level during the review process. This Standard recognizes that meeting R&M objectives in a comprehensive endeavor that is achieved in an interdisciplinary manner in the execution of program and project activities over the lifecycle in cooperation with the Systems Engineering of the program and project.

1.1.3 While this document may give guidance with processes associated with the objectives, it is generally not the intent of this Standard to prescribe particular processes, rather to allow programs and projects to select effective means of incorporating R&M considerations into their activities and to enable innovation. Guidance is provided to help programs, projects, contractors, and providers select appropriate processes and methods. Additional guidance may be issued in the form of handbooks or technical bulletins.

1.2 Applicability

1.2.1 This Standard is approved for use by NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers, and may be cited in contract, program, and other Agency documents as a technical requirement. This Standard may also apply to the Jet Propulsion Laboratory (JPL) or to other contractors, grant recipients, or parties to agreements only to the extent specified or referenced in their contracts, grants, or agreements.

1.2.2 This Standard does not apply to facility projects except for critical technical facilities specifically developed or significantly modified for Space Flight Systems as identified in NPR

7120.5. Implementation of R&M on facilities is in accordance with NPD 8831.1. Maintenance of Institutional and Program Facilities and Related Equipment; NPR 8820.2, Facility Project Requirements; NPR 8831.2, Facilities Maintenance Management; NASA Reliability Centered Maintenance Guide for Facilities and Collateral Equipment; and NASA Reliability Centered Building and Equipment Acceptance Guide.

2. APPLICABLE DOCUMENTS

2.1 General

The documents listed in this section contain provisions that constitute requirements of this Standard as cited in the text. Use of more recent issues of cited documents may be authorized by the responsible Technical Authority. The applicable documents are accessible via the NASA Technical Standards System at http://standards.nasa.gov, http://nodis3.gsfc.nasa.gov/ or may be obtained directly from the Standards Developing Organizations or other document distributors.

2.2 Government Documents

NPR 7120.5	NASA Space Flight Program and Project Management Requirements

2.3 Non-Government Documents

None

2.4 Order of Precedence

This NASA Technical Standard establishes requirements for the Reliability and Maintainability Engineering technical disciplines but does not supersede nor waive established Agency requirements found in other documentation. Conflicts between this Standard and other requirements documents shall be resolved by the responsible Technical Authority.

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

CIL	Critical Item List
DC	Direct Current
EMC	Electromagnetic Compatibility
ESD	Electrostatic Discharge
ESS	Environmental Stress Screening
FMEA	Failure Modes and Effects Analysis

FMECA	Failure Modes, Effects, and Criticality Analysis
FRACAS	Failure Reporting and Corrective Action System
FTA	Fault Tree Analysis
GIDEP	Government-Industry Data Exchange Program
GPMC	Governing Program Management Council
HALT	Highly Accelerated Life Testing
HAST	Highly Accelerated Stress Testing
IESD	Internal Electrostatic Discharge
I&T	Integration and Test
JPL	Jet Propulsion Laboratory
LOC	Loss of Crew
LOM	Loss of Mission
MDT	Mean Downtime
MMH	Maintenance Man-Hour
MMOD	Micrometeoroids and Orbital Debris
MTA	Maintenance Task Analysis
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
OSMA	Office of Safety and Mission Assurance
PDR	Preliminary Design Review
P/F/A	Problems/Failures/Anomalies
PMC	Program Management Council

PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action System
PSA	Parts Stress Analysis
R&M	Reliability and Maintainability
RBD	Reliability Block Diagram
RBDA	Reliability Block Diagram Analysis
RCM	Reliability-Centered Maintenance
RMA	Reliability, Maintainability, and Availability
SEE	Single Event Effects
SMA	Safety and Mission Assurance
TRL	Technical Readiness Level
WCA	Worst Case Analysis

3.2 Definitions

The following definitions may be used to plan R&M activities and interpret the R&M considerations outlined in Appendix A.

Anomaly: An unexpected event that is outside of certified design/performance specification limits or expectations.

Availability, Operational (A_o): The percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission and can be expressed as uptime/(uptime+downtime). It includes logistics time, ready time, and waiting or administrative downtime, and both preventive and corrective maintenance downtime. This value is equal to the Mean Time Between Failure (MTBF) divided by the MTBF plus the Mean Downtime (MDT). This measure extends the definition of availability to elements controlled by the logisticians and mission planners such as quantity and proximity of spares to the hardware item. A_o is the quantitative link between readiness objectives and supportability.

Availability, Inherent (A_i): The percentage of time that a system or group of systems within a unit are operationally capable of performing an assigned mission with respect only to operating time and corrective maintenance time. It excludes logistics time, waiting or administrative downtime, and preventive maintenance downtime. It includes corrective maintenance downtime. Inherent availability is generally derived from analysis of an engineering design and is calculated as the Mean Time To Failure

(MTTF) divided by the MTTF plus the Mean Time To Repair (MTTR). It is based on quantities under control of the designer.

Contract: An agreement between two or more parties, which is normally written and enforceable by law.

Contractor: A party under contract to provide a product or service at a specified cost to another party (or parties) to the contract, also known as the customer(s).

Criticality (of a failure): A measure of the significance or severity of a failure on mission performance, hazards to material or personnel, and maintenance cost. Programs/projects typically establish their own criticality definitions and classifications.

Dependability: The ability to avoid service failures that are more frequent and more severe than is acceptable.

Environment: The natural and induced conditions experienced by a system including its people, processes, and products during operational use, stand-by, maintenance, transportation, and storage.

Failure: [1] Inability of a system, subsystem, component, or part to perform its required function within specified limits. [2] Non-performance or incorrect performance of an intended function of a product. A failure is often the manifestation of one or more faults and is permanent.

Failure Analysis: The conduct of evaluations and analyses to determine the specific cause of system (including elements of hardware, software, and human performance) and/or component failure.

Failure Cause: The defect in design, process, quality, or part application that is the underlying cause of a failure or which initiates a process that leads to failure.

Failure Effect: The immediate consequence of a failure on operation, function or functionality.

Failure Mechanism: The process (e.g., physical, chemical, electrical, thermal) of degradation or the chain of events, which results in a particular failure mode.

Failure Mode: [1] Particular way in which a failure can occur, independent of the reason for failure. [2] The characteristic manner in which a failure occurs, independent of the reason for failure; the condition or state that is the end result of a particular failure mechanism; the consequence of the failure mechanism through which the failure occurs, e.g., short, open, fracture, excessive wear.

Failure Modes and Effects Analysis (FMEA): [1] A bottoms up systematic, inductive, methodical analysis performed to identify and document all identifiable failure modes at a prescribed level and to specify the resultant effect of the modes of failure. It is usually performed to identify critical single failure points in hardware. In relation to formal hazard analyses, FMEA is a subsidiary analysis. [2] A bottom-up systematic, inductive, methodical analysis performed to identify and document all identifiable failure modes at a prescribed level and to specify the resultant effect of the modes of failure. [3] Analysis of a system and the working interrelationships of its elements to determine ways in which failures can occur (failure modes) and the effects of each potential failure on the system element in which it occurs, on other system elements, and on the mission.

Failure Mode Effects and Criticality Analysis (FMECA): Analysis of a system and the working interrelationships of its elements to determine ways in which failures can occur (failure modes) and the effects of each potential failure on the system element in which it occurs, on other system elements, and on the mission, and the study of the relative mission risk or criticality of all potential failure modes.

Failure Propagation: Any physical or logical event caused by failure within a product which can lead to failure(s) of products outside the boundaries of the product under analysis.

Failure Tolerance: The ability to perform a function in the presence of any of a specified number of coincident, independent failure causes of specified types.

Fault: [1] An undesired system state and/or the immediate cause of failure (e.g., maladjustment, misalignment, defect, or other). The definition of the term "fault" envelopes the word "failure," since faults include other undesired events such as software anomalies and operational anomalies. [2] An inherent defect in a product which may or may not ever manifest, such as a bug in software code.

Fault Isolation: The process of determining the approximate location of a fault.

Fault Management: The engineering process that encompasses practices which enable an operational system to contain, prevent, detect, isolate, diagnose, respond to, and recover from conditions that may interfere with nominal mission operations.

Fault Propagation: The propagation of effects seen from one fault into other faults and potentially failures.

Fault Tree Analysis (FTA): A deductive system reliability tool that provides both qualitative and quantitative measures of the probability of failure. It estimates the probability that a top-level event will occur, systematically identifies all possible causes leading to the top event, and documents the analytic process to provide a baseline for future studies of alternative designs.

Hardware: Items made of a material substance but excluding computer software and technical documentation.

Level of Repair Analysis (LORA): An analytical methodology used to assist in developing maintenance concepts and establishing the maintenance level at which components will be replaced, repaired, or discarded based on economic/noneconomic constraints and operational readiness requirements. Also known as an Optimum Repair Level Analysis (ORLA).

Maintainability: A measure of the ease and rapidity with which a system or equipment can be restored to operational status. It is characteristic of equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed. One expression of maintainability is the probability that an item will be retained in or restored to a specified condition within a given period of time, when the maintenance is performed in accordance with prescribed procedures and resources.

Maintenance: All actions necessary for retaining an item in, or restoring it to, a specified condition.

Maintenance Analysis: The process of identifying required maintenance functions by analysis of the design, and to determine the most effective means to accomplish those functions.

Milestone: Any significant event in the program/project life cycle or in the associated reliability or maintainability program that is used as a control point for measurement of progress and effectiveness or for planning or redirecting future effort.

Mission Critical: [1] Item or function that must retain its operational capability to assure no mission failure (i.e., for mission success). [2] An item or function, the failure of which may result in the inability to retain operational capability for mission continuation if a corrective action is not successfully performed.

Mitigation: An action taken or planned to reduce the consequence of an event (synonyms: compensating provisions, fault-tolerance).

Operational Readiness: The ability of a system to respond and perform its mission upon demand.

Prevention: An action taken to reduce the likelihood of an event (Synonyms: preventive measure, fault avoidance).

Problem/Failure/Anomailies Management (P/F/A): A formalized process to document, resolve, verify, correct, review and archive P/F/A incurred during the development of functional hardware or software.

Program: An activity within an Enterprise having defined goals, objectives, requirements, funding, and consisting of one or more projects, reporting to the NASA Program Management Council (PMC), unless delegated to a Governing Program Management Council (GPMC).

Project: An activity designated by a program and characterized as having defined goals, objectives, requirements, Life Cycle Costs, a beginning, and an end.

Redundancy: Use of more than one independent means to accomplish a given function.

Redundancy (of design): A design feature which provides a system with more than one function for accomplishing a given task so that more than one function must fail before the system fails to perform the task. Design redundancy requires that a failure in one function does not impair the system's ability to transfer to a second function.

Reliability: The probability that an item will perform its intended function for a specified interval under stated conditions. The function of an item may be composed of a combination of individual subfunctions to which the top-level reliability value can be apportioned.

Reliability Analyses: A set of conceptual tools and activities used in reliability engineering. Examples of common analyses are Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis in failure space and Reliability Block Diagram Analysis (RBDA) in success space.

Reliability Assurance: The management and technical integration of the reliability activities essential in maintaining reliability performance, including design, production, risk management, and product assurance activities.

Reliability Block Diagram Analysis (RBDA): A deductive (top-down) method that generates a symbolic-logic model in success space that depicts and analyzes the reliability (and/or availability) relationships between the system and system elements and/or events. Typical RBD models are constructed of series, parallel, and/or combinations of series and parallel configurations. The RBD model describes a successful operation when an uninterrupted path exists between the model's input and output. The RBDA process, for example, provides a design baseline and serves as a means to identify weak areas and changes early in the design phase and serves as input to accomplish related analyses (e.g., FMEA, FTA, spare, and maintenance).

Reliability Centered Maintenance: An on-going process that determines the mix of corrective and preventive maintenance practices to provide the required reliability at the minimum cost. It can use diagnostic tools and measurements to assess when a component is near failure and should be replaced. The basic thrust is to eliminate more costly corrective maintenance and minimize preventive maintenance.

Requirements: Requirements are statements of need that define what a system will do and how well it must perform those tasks.

Review: A critical examination of a task or program/project to determine compliance with requirements and objectives.

Risk: In the context of mission execution, risk is operationally defined as a set of triplets. [1] The *scenario(s)* leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage). [2] The *likelihood(s)* (qualitative or quantitative) of those scenarios. [3] The *consequence(s)* (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur. Uncertainties are included in the evaluation of likelihoods and consequences.

Risk Acceptance: The formal process of justifying and documenting a decision not to mitigate a given risk associated with achieving given objectives or given performance requirements.

Risk Management: An organized, systematic decision-making process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk and establishes mitigation approaches and plans to increase the likelihood of achieving program/project goals.

Risk Reduction: The modification of a process, system, or activity in order to reduce a risk by reducing its probability, consequence severity, or uncertainty, or by shifting its timeframe.

Safety Critical Event: An event (successful or failure) of whose proper recognition, control, performance or tolerance is essential to safe system operation or use.

Severity (of a failure): A measure of the effect or consequence of a failure in relation to mission performance, hazards to material or personnel, and maintenance cost. Programs/projects typically establish their own severity definitions and classifications.

Single Point Failure: An independent element of a system (hardware, software, or human), the failure of which would result in loss of objectives, hardware, or crew.

Spares: Maintenance replacements for parts, components, or assemblies in deployed items of equipment.

Stress Screening: The process of applying mechanical, electrical, or thermal stresses to an equipment item for the purpose of precipitating latent part and workmanship defects to early failure.

Subsystem: A grouping of items satisfying a logical group of functions within a system.

Supplier: Any organization, which provides a product or service to a customer. By this definition, suppliers may include vendors, subcontractors, contractors, flight programs/projects, and the NASA organization supplying science data to a principal investigator. (In contrast, the classical definition of a supplier is: a subcontractor, at any tier, performing contract services or producing the contract articles for a contractor.).

Support Equipment: Equipment required to maintain systems in effective operating condition in its intended environment, including all equipment required to maintain and operate the system and related software.

Sustainability: The ability to maintain the necessary level and duration of logistics support to achieve mission objectives.

Sustainment: The provision of logistics and personnel services required to maintain and prolong operations until successful mission accomplishment.

System: [1] The combination of elements that function together to produce the capability to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose. [2] The end product (which performs operational functions) and enabling products (which provide life-cycle support services to the operational end products) that make up a system.

Tailoring: The process used to adjust or seek relief from a prescribed requirement to accommodate the needs of a specific task or activity (e.g., program or project). The tailoring process results in the generation of deviations and waivers depending on the timing of the request (Source: NPR 7120.5, NASA Space Flight Program and Project Management Requirements).

Task: A function to be performed. In contract proposals, a unit of work that is sufficiently well defined so that, within the context of related tasks, readiness criteria, completion criteria, cost and schedule can all be determined.

Test: A procedure for critical evaluation; a means of determining the presence, quality, or truth of something; a trial. In engineering, a method of determining performance by exercising or operating a system or item using instrumentation or special test equipment that is not an integral part of the item being tested.

Testability: A design characteristic that permits timely and cost-effective determination of the status (operable, inoperable or degraded) of a system or subsystem with a high level of confidence. Testability attempts to quantify those attributes of system design that facilitate detection and isolation of faults that affect system performance.

Validation: To establish the soundness of, or to corroborate. As a process, validation answers, "Are we building the right system?" Validation testing of products is performed to ensure that each reflects an accurate interpretation and execution of requirements and meets a level of functionality and performance that is acceptable to the user or customer.

Verification: The task of determining whether a system or item meets the requirements established for it. As a process, verification answers, "Are we building the system right?"

4. R&M REQUIRED APPROACH

4.1 R&M Technical Objectives

4.1.1 The top-level objective of R&M activities in NASA support systems programs and projects is to ensure that systems perform as required over their lifecycles to satisfy mission objectives including safety, reliability, maintainability, and quality assurance requirements as defined in the references listed in Appendix D.

4.1.2 Programs and projects are expected to address this objective by conducting analysis and testing activities and making the necessary design and operational choices to limit the likelihood of faults and failures, and to provide mitigation and restoration capabilities as needed to maintain an acceptable level of functionality considering those safety, performance, and reliability objectives.

4.1.3 Accordingly, the top-level objective is decomposed into the following four subobjectives:

a. The system conforms to the design intent (interfaces and/or functions) and performs as planned under nominal and failed conditions.

b. The system and its elements remain functional for the intended lifetime, environment, operating conditions, and usage.

c. The system is tolerant to faults, failures, and other anomalous internal and external events.

d. The system has an acceptable level of reliability and maintainability in order to properly satisfy the availability requirement.

4.1.4 This Standard specifies strategies to meet each of these objectives. The strategies represent suggested guidance for spaceflight programs and projects that can allow tailoring per risk classification and acceptable risk posture. The decomposition of top-level objectives into strategies is listed in Appendix A. The strategies represent minimum expectations for R&M activities in NASA's spaceflight programs and projects.

4.2 Objectives-Driven Approach

4.2.1 The intent of this Standard is to provide the key R&M objectives, rather than a fixed set of R&M products and processes, and provide the necessary flexibility to address those key objectives consistent with governing acquisition, management, and engineering approaches, and commensurate with risk tolerance.

4.2.2 Programs and projects, as part of their planning activities, shall identify how they intend to address the R&M objectives, implement the associated strategies, and evaluate evidence of successful implementation.

5. IMPLEMENTATION REQUIREMENTS

5.1 Planning and Implementation

5.1.1 The Project or Program shall establish and implement R&M requirements in the SMA Plan required in NPR 7120.5. The SMA Plan should address the objectives and strategies in Appendix A and listed in the tables of Appendix B of this NPR. Some relevant activities necessary to address the objectives may be performed by projects or programs that are not within the scope of the R&M practitioner or managed within the discipline of R&M. However, all the objectives and strategies herein are relevant to project and program reliability and mission success. Programs and projects shall ensure the appropriate interfaces are coordinated among the relevant stakeholders. Programs and projects are encouraged to take an interdisciplinary approach consistent with Systems Engineering in planning to meet R&M objectives and strategies.

5.1.2 The R&M requirements and plan shall specify and/or reference other appropriate program or project plans, documents or models, relevant to the following:

a. R&M criteria, including those derived from safety, mission success, MMOD or sustainment;

b. Functional and performance objectives and requirements plans, documents or models in order to enable the performance of effective R&M activities such as quantitative reliability models and Failure Modes and Effects Analysis (FMEA);

c. Applicable design and process Standards impacting system reliability so as to enable effective performance of R&M activities including Failure Modes and Effects Analysis (FMEA) and the development of Critical Items Lists (CIL);

d. The scope of each activity, commensurate with the minimum scope of strategy implementation specified in the tables of Appendix B;

e. The products that will be used as evidence for the strategies that were implemented and objectives addressed, including any alternatives to the referenced evidentiary methods provided in the tables of Appendix B;

f. Instances where R&M products serve as design requirement verification;

g. A schedule of R&M products and deliverables consistent with Project or Program design, developmental, and operational milestone criteria;

h. Organizations and organizational interfaces and processes (e.g., risk management) involved in the execution of the activities;

i. The strategy for independent evaluation of R&M products and activities where applicable and commensurate with the minimum scope of strategy implementation.

j. Lessons learned, best practices and system heritage throughout the life cycle.

5.1.3 The Project or Program shall obtain concurrence from the SMA Technical Authority that the Project or Program requirements and plan of activities, or any update thereof, are sufficient to address the R&M objectives and strategies commensurate with the mission class.

5.1.4 The Project or Program shall identify, in an appropriate planning document, the organizations that are responsible for the provision of personnel, funding, tools, and other resources needed to satisfy the R&M requirements and plan.

5.2 Evaluation and Review

5.2.1 The SMA Technical Authority shall verify that the strategy for independent evaluation of R&M products and activities is implemented.

5.2.2 At milestone reviews, the Project or Program, with concurrence from the SMA Technical Authority, shall provide evidence and/or present R&M results that show:

a. R&M objectives and strategies have been adequately addressed consistent with the plan;

b. R&M products are at an appropriate maturity level and meet applicable Standards;

c. Related technical risks have been identified and are deemed to be acceptable.

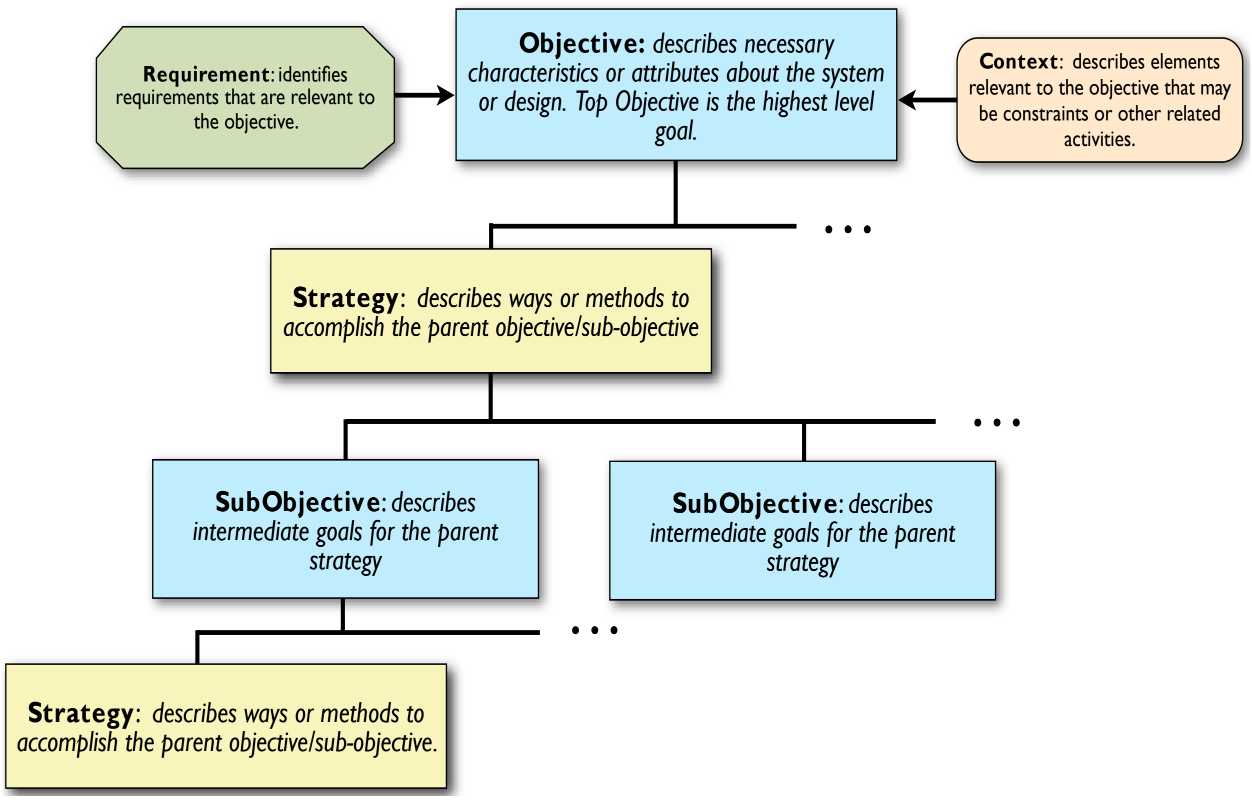
5.2.3 At readiness reviews, the Project or Program, with concurrence from the SMA Technical Authority, shall confirm that:

a. R&M objectives and strategies have been adequately addressed;

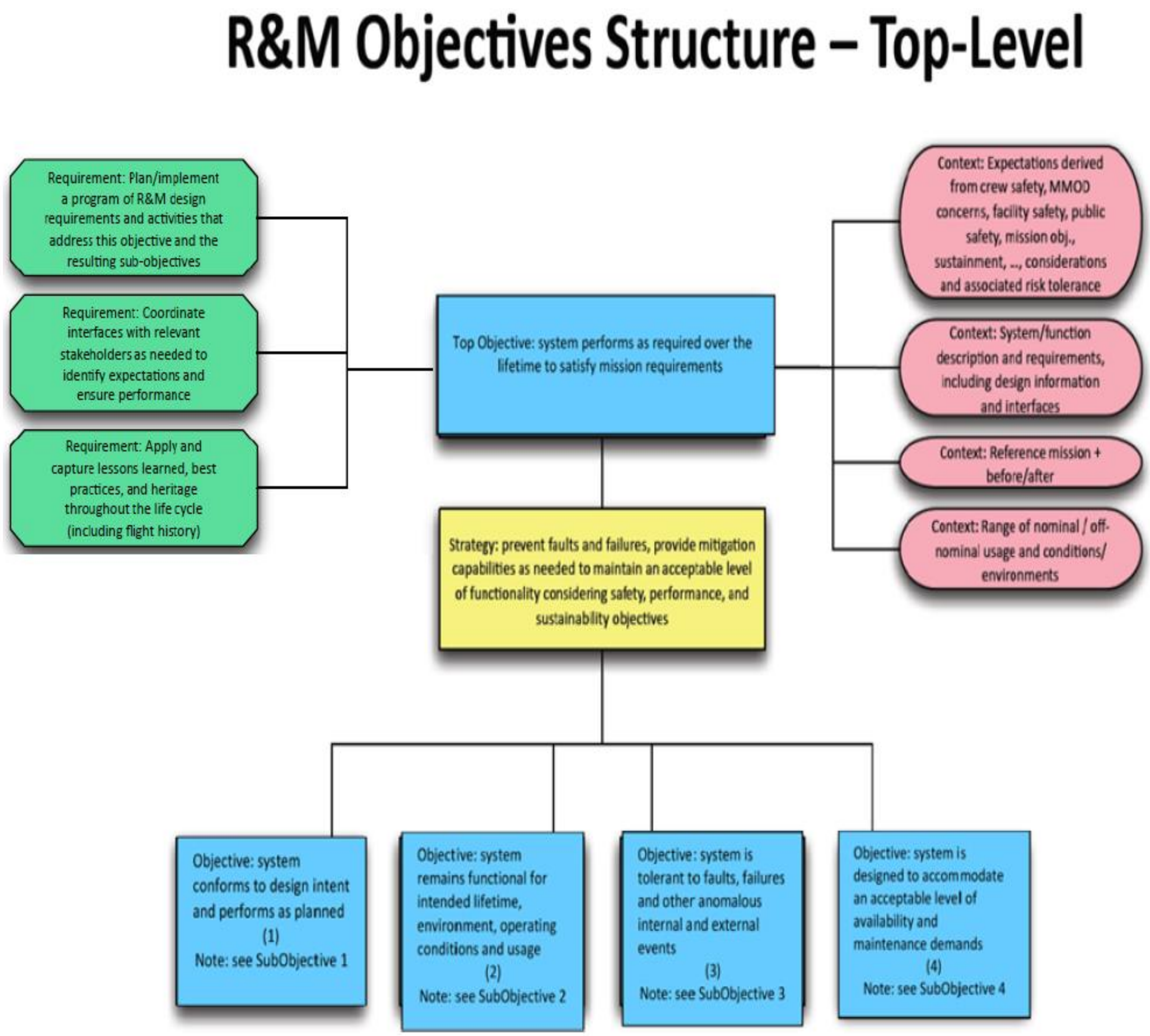
b. Related residual risks are deemed to be acceptable.

APPENDIX A. R&M OBJECTIVES HIERARCHY

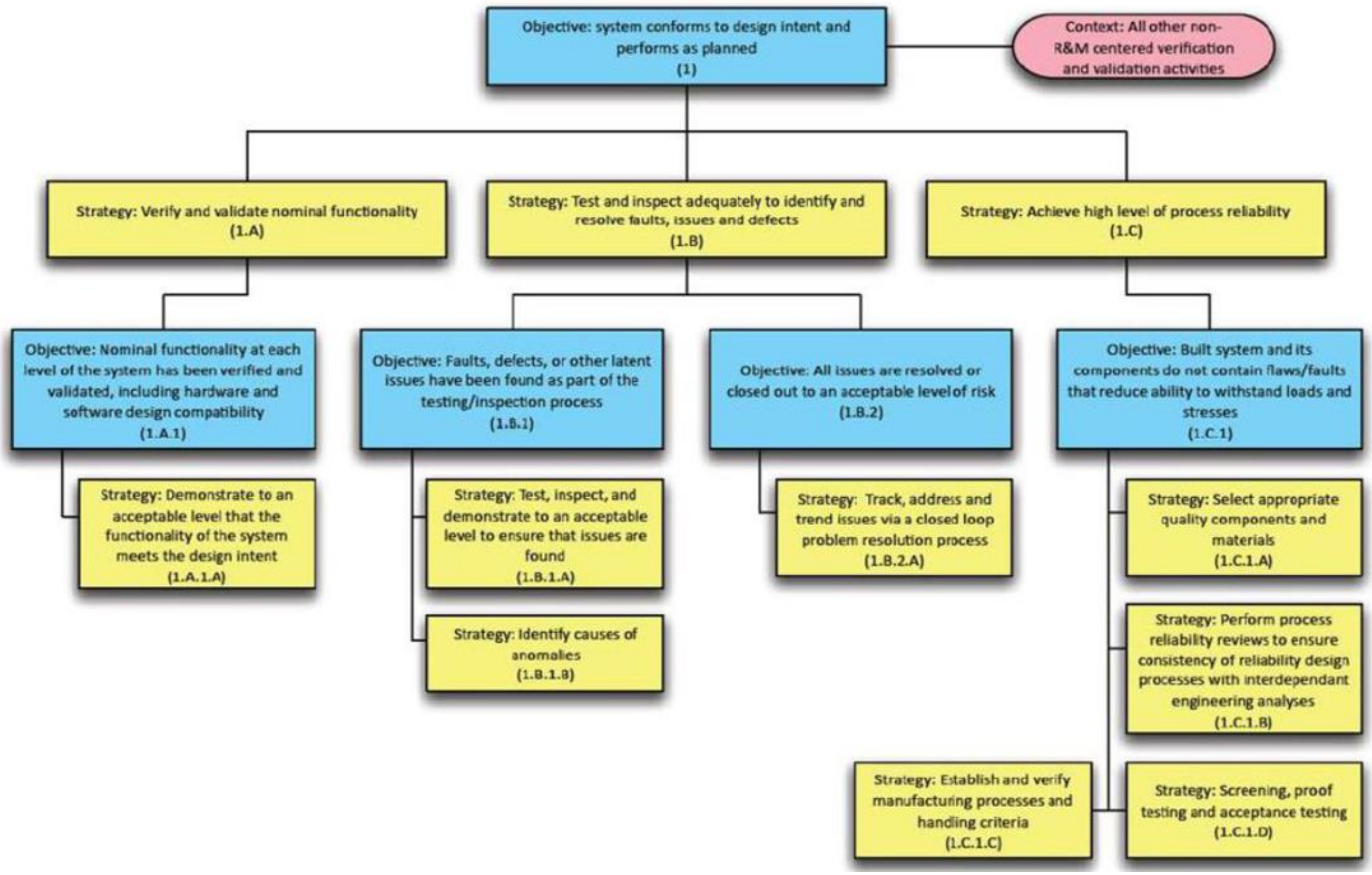
The following pages contain a flowchart view of the R&M objectives hierarchy. The format defines objectives and subobjectives while mapping them with strategies that are used to accomplish the objectives. Subobjectives are used to further elaborate on top-level objectives, but each objective block uses at least one strategy to accomplish it. As a benefit that is in line with the intent of this standard, this method clearly describes the objectives and strategies and separates them accordingly.



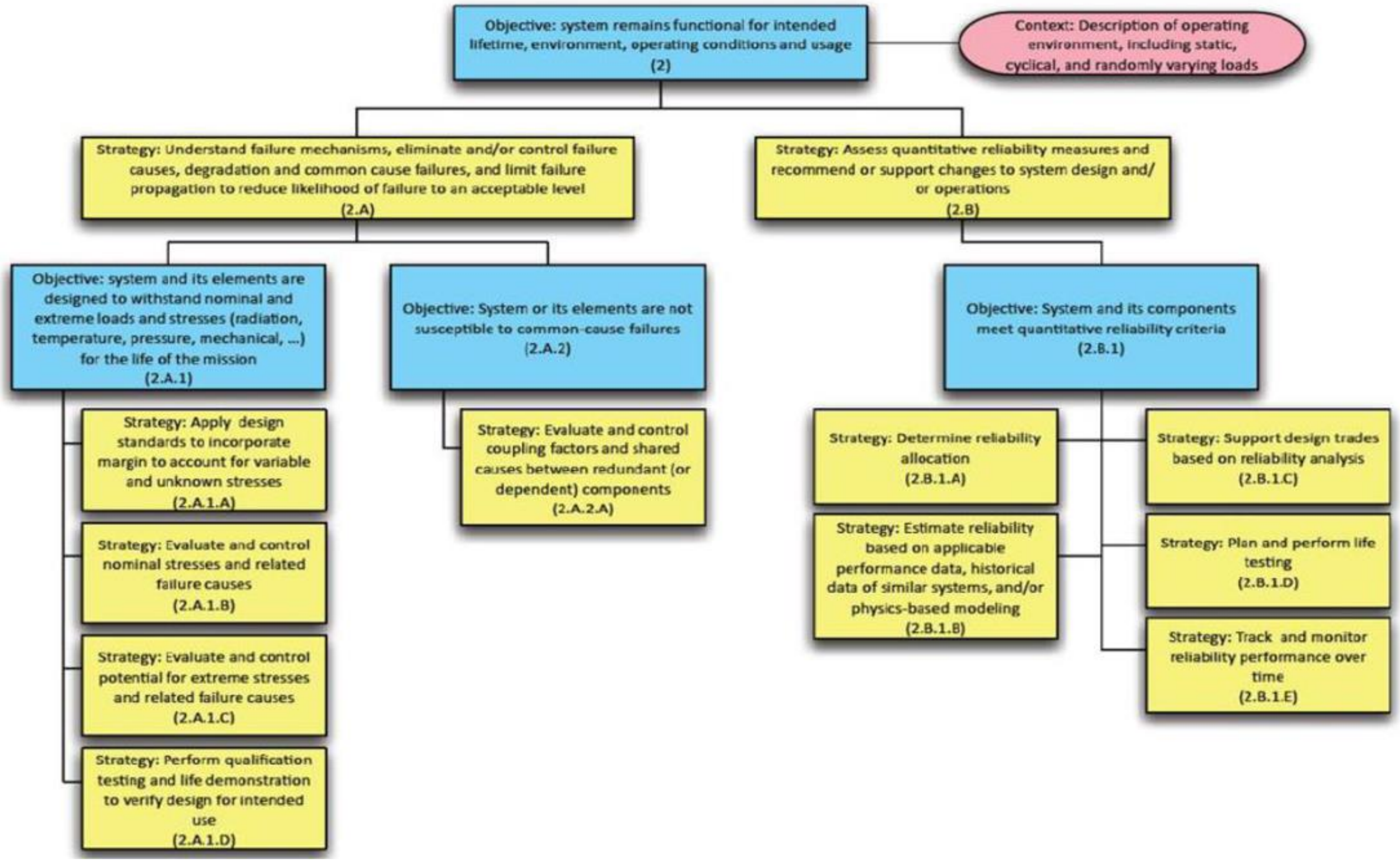
The hierarchy uses these two essential blocks in an alternating fashion; i.e., each objective is coupled with at least one strategy and then each sub objective of that pair is coupled with at least one strategy. In addition to these two primary blocks, the notation used herein includes some "Context" blocks that are used solely as descriptive tags to Objective or Strategy blocks. These will be used purely to define context elements of a primary block.


R&M Objectives Structure – Top-Level
Requirement: Plan/implement a program of R&M design requirements and activities that address this objective and the resulting sub-objectives
Requirement: Coordinate interfaces with relevant stakeholders as needed to identify expectations and ensure performance
Requirement: Apply and capture lessons learned, best practices, and heritage throughout the life cycle (including flight history)
Top Objective: system performs as required over the lifetime to satisfy mission requirements
Context: Expectations derived from crew safety, MMOD concerns, facility safety, public safety, mission obj., sustainment, ..., considerations and associated risk tolerance
Context: System/function description and requirements, including design information and interfaces
Context: Reference mission + before/after
Context: Range of nominal / off-nominal usage and conditions/ environments
Strategy: prevent faults and failures, provide mitigation capabilities as needed to maintain an acceptable level of functionality considering safety, performance, and sustainability objectives
Objective: system conforms to design intent and performs as planned (1) Note: see SubObjective 1
Objective: system remains functional for intended lifetime, environment, operating conditions and usage (2) Note: see SubObjective 2
Objective: system is tolerant to faults, failures and other anomalous internal and external events (3) Note: see SubObjective 3
Objective: system is designed to accommodate an acceptable level of availability and maintenance demands (4) Note: see SubObjective 4

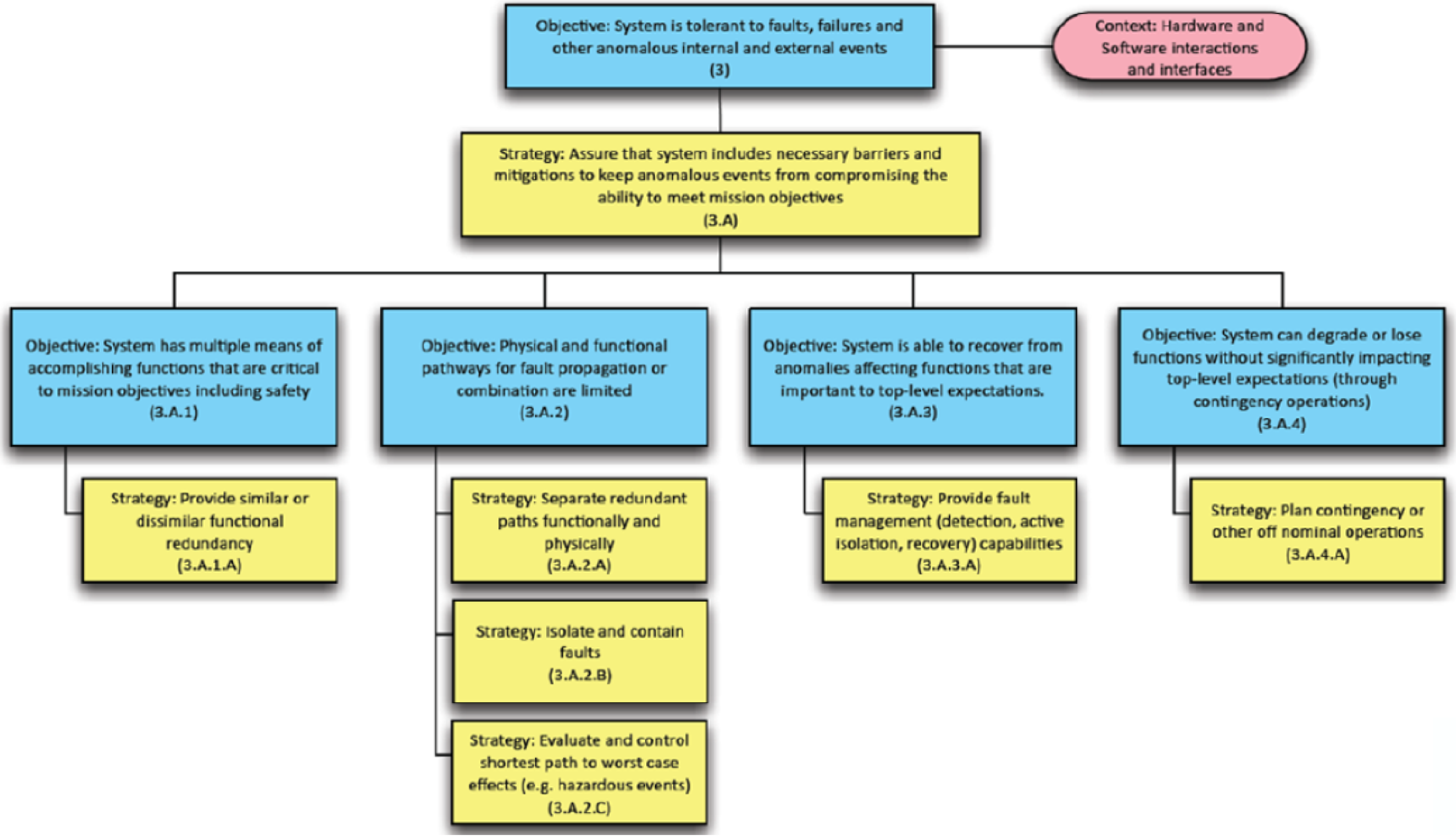
SubObjective 1: System Conforms to Design Intent and Performs as Planned



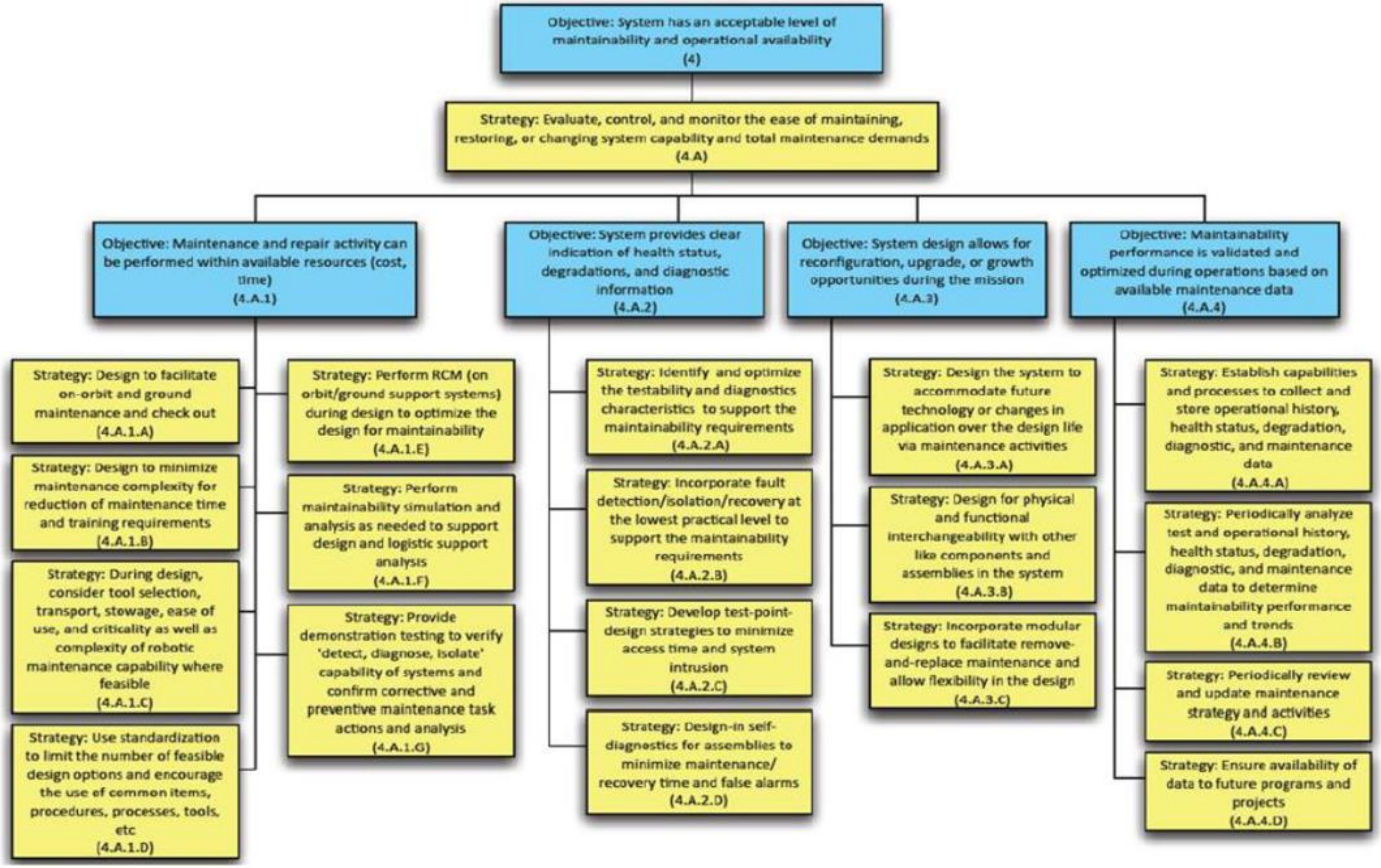
SubObjective 2: System Remains Functional for Intended Lifetime, Environment, Operating Conditions and Usage



SubObjective 3: System is Tolerant to Faults, Failures and Other Anomalous Internal and External Events



SubObjective 4: System Has an Acceptable Level of Maintainability and Operational Availability



APPENDIX B. R&M OBJECTIVES HIERARCHY WITH SCOPE IDENTIFICATION

The following pages contain a tabular view of the R&M objectives hierarchy with information added regarding the evidentiary methods to be used to satisfy objectives, as well as the scope to which those methods should be performed for various mission classes. The "evidence" column suggests the type of methodologies that may be used to satisfy the corresponding R&M objective when formulating an R&M Plan for a program or project (see section 5). This evidentiary information is provided for each bottom-level strategy in the objectives hierarchy. Along with this information about evidence are some scope definitions. In general, the scope for each piece of evidence is suggested for the top-level mission class (human spaceflight or class A robotic missions), and then it may be reduced as applicable for higher risk mission classes.

			Scope						
		Evidence	Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
1.A	Strategy: Verify and validate nominal functionality								
1.A.1	Objective: Nominal functionality at each level of the system has been verified and validated, including hardware and software design compatibility								
1.A.1.A	Strategy: Demonstrate to an acceptable level that the functionality of the system meets the design intent	Verification and Validation Testing	Test for nominal functionality per systems engineering process requirements for the applicable mission class.						
1.B	Strategy: Test and inspect adequately to identify and resolve faults, issues and defects								
1.B.1	Objective: Faults, defects, or other latent issues have been found as part of the testing/inspection process								
1.B.1.A	Strategy: Test, inspect, and demonstrate to an acceptable level to ensure that issues are found	Testing and Analysis Methods such as: Sneak circuit analysis, EMC emissions test, EMC isolation test, EMC susceptibility test, ESD discharge test, HALT, HAST, Life testing, Regression Testing, Stress Testing, Static Code Analysis	Test for all functions			Hybrid of Class B and Class D scope selected on case by case basis.	Test for mission-critical functions		For flight operations, functions critical to health management, safe hold, and data related to public safety
1.B.1.B	Strategy: Identify causes of anomalies	PRACA/FRACAS, Other Failure Analysis (Root Cause Analysis, Fishbone Analysis, Fault Tree Analysis, Destructive Physical Analysis, etc.)	Problems/Failures/Anomalies critical to all functions			Problems/Failures/Anomalies critical to mission functions			Problems/Failures/Anomalies affecting flight operations, functions critical to health management, safe hold, and data related to public safety
1.B.2	Objective: All issues are resolved or closed out to an acceptable level of risk								
1.B.2.A	Strategy: Track, address and trend issues via a closed loop problem resolution process	PRACA/FRACAS	All Problems/Failures/Anomalies involving flight hardware and any nonflight hardware that has a physical or functional interface with flight hardware				Problems/Failures/Anomalies critical to safety, and mission success. No formal reporting for P/F/As relating to mission success		

			Scope						
		Evidence	Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
1.C	Strategy: Achieve high level of process reliability								
1.C.1	Objective: Built system and its components do not contain flaws/faults that reduce ability to withstand loads and stresses								
1.C.1.A	Strategy: Select appropriate quality components and materials	approved parts list, parts control and traceability, materials review	Parts/materials control standards applicable to Human Space Flight	Parts/materials control standards applicable to individual mission class				Parts/materials control standards applicable to research and technology	Parts/materials control standards applicable to ground based systems, if they exist
1.C.1.B	Strategy: Perform process reliability reviews to ensure consistency of reliability design processes with interdependent engineering analyses	technical oversight & management, independent technical review, peer technical review, software process audits	High rigor review of all reliability design processes and engineering analyses			Selective review of reliability design processes and engineering analyses based on high risk drivers			For telemetry items, same scope as Class A/B. For other items, selective review as in Class C/D
1.C.1.C	Strategy: Establish and verify manufacturing processes and handling criteria	approved parts list, ground handling analysis, process variance analysis, process FMEA, ground handling test, process capability assessment	Parts control handling standards and manufacturing criteria applicable to Human Space Flight	Parts control handling standards and manufacturing criteria applicable to individual mission class				Parts control handling standards and manufacturing criteria applicable to research and technology	Parts control handling standards and manufacturing criteria applicable to ground based systems, if they exist
1.C.1.D	Strategy: Screening, proof testing and acceptance testing	Environmental Stress Screening, Inspection Criteria, Acceptance Test Plan	Test/Screen at full level of rigor (duration, number of cycles, etc. for ESS). Test/Screen will be tailored based on criticality				Test/Screen at decreased level of rigor than lower risk classes (box level). Test/Screen will be tailored based on criticality		Verify functionality of ground support equipment used for testing. Screen/proof testing of safety elements

		Evidence	Scope: Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
2.A	Strategy: Understand failure mechanisms, eliminate and/or control failure causes, degradation and common cause failures, and limit failure propagation to reduce likelihood of failure to an acceptable level								
2.A.1	Objective: System and its elements are designed to withstand nominal and extreme loads and stresses (radiation, temperature, pressure, mechanical, ...) for the life of the mission								
2.A.1.A	Strategy: Apply design standards to incorporate margin to account for variable and unknown stresses	Derating, structural safety margins, thermal, aging, radiation design margins	Apply class-specific design margins (structural, thermal, etc.)						
2.A.1.B	Strategy: Evaluate and control nominal stresses and related failure causes	Parts stress analyses, structural/thermal analyses, surface charging/ESD	Demonstrate compliance with margins to class-specific level of detail						
2.A.1.C	Strategy: Evaluate and control potential for extreme stresses and related failure causes	Worst Case Analysis, parts stress analyses, structural/thermal analyses, Single Event Effect Analysis, physics of failure analysis, radiation dose analysis, ground handling test	Demonstrate compliance with margins to class-specific level of detail						
2.A.1.D	Strategy: Perform qualification testing and life demonstration to verify design for intended use	Test Results, Life Analysis, Fatigue Analysis, Worst Case Analysis, acoustic test, constant acceleration test, HALT, HAST, magnetic test, mechanical shock test, powered-on vibration test, pyrotechnic shock test, random vibration test, sine dynamic test, Structural Proof Loading Test, thermal testing, thermal test, voltage/temperature margin test	Demonstrate class-specific positive safety margins and specific safety factors consistent with requirements based on material, function, environment and flight dynamics (where applicable)						
2.A.2	Objective: System or its elements are not susceptible to common-cause failures								
2.A.2.A	Strategy: Evaluate and control coupling factors and shared causes between redundant (or dependent) components	Fault Tree, FMEA	Control to preserve redundancy level compliant with mission class.						Suitable to meet required system needs

			Scope						
		Evidence	Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
2.B	Strategy: Assess quantitative reliability measures and recommend or support changes to system design and/or operations								
2.B.1	Objective: System and its components meet quantitative reliability criteria								
2.B.1.A	Strategy: Determine reliability allocation	Allocation Analysis	Perform reliability allocation consistent with LOC/LOM requirement	Perform reliability allocation consistent with LOM requirement					Perform reliability allocation to appropriate level to support maintainability and availability requirement
2.B.1.B	Strategy: Estimate reliability based on applicable performance data, historical data of similar systems, and/or physics-based modeling	Quantitative Reliability Modeling and Analysis	Perform reliability performance assessment to support LOC/LOM assessment	Perform reliability performance assessment to support LOM assessment					Perform reliability performance assessment to appropriate level to support maintainability and availability requirement
2.B.1.C	Strategy: Support design trades based on reliability analysis	Trade Study Analysis	As required to support mission, functional, and performance requirements						
2.B.1.D	Strategy: Plan and perform life testing	Life testing, Demonstration Testing	As required to support mission, functional, and performance requirements						
2.B.1.E	Strategy: Track and monitor reliability performance over time	Performance Trending Analysis, Failure Trending Analysis, Reliability Growth Modeling	Perform analysis and trending as indicated and as appropriate to mission type and class						

			Scope						
		Evidence	Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
3.A	Strategy: Assure that system includes necessary barriers and mitigations to keep anomalous events from compromising the ability to meet mission objectives								
3.A.1	Objective: System has multiple means of accomplishing functions that are critical to mission objectives including safety								
3.A.1.A	Strategy: Provide similar or dissimilar functional redundancy	Redundancy RBD/FTA/FMECA (with mitigation and detection analysis)	Perform redundancy decomposition consistent with program-defined redundancy requirements						
3.A.2	Objective: Physical and functional pathways for fault propagation or combination are limited								
3.A.2.A	Strategy: Separate redundant paths functionally and physically	FMEA, FMECA	All safety critical and mission critical functions where redundancy exists			All safety critical functions where redundancy exists			
3.A.2.B	Strategy: Isolate and contain faults	Design Requirement Verification Matrix, FMECA	Faults or failures that would result in a catastrophic or mission critical event (including failure of non-critical functions that could result in a single point failure)			Faults or failures that would result in a safety critical event, loss of a redundant string, or progagtion of faults from non-critical failures		Faults or failures that would result in a safety critical event	Faults or failures that would result in a safety critical event, or any propagation to flight equipment
3.A.2.C	Strategy: Evaluate and control shortest path to worst-case effects (e.g. hazardous events)	Fault Tree Analysis, FMEA, FMECA, Hazard Analysis	Any combination of failures that could lead to safety critical events/LOC/LOM consistent with program-defined failure tolerance requirements	Any combination of failures that could lead to safety critical events/LOM consistent with program-defined failure tolerance requirements		Any combination of failures that could lead to safety critical event consistent with program-defined failure tolerance requirements			Any combination of failures that could lead to safety critical event or propagation to flight equipment consistent with program-defined failure tolerance requirements
3.A.3	Objective: System is able to recover from anomalies affecting functions that are important to top-level expectations								
3.A.3.A	Strategy: Provide fault management (detection, active isolation, recovery) capabilities	FMEA, FMECA, Hazard Analysis, Ambiguity Matrix, FTA	Faults that could affect critical and catastrophic functions	Faults that could affect critical functions and functions protecting from safety critical events				Faults that could affect functions protecting from safety critical events	Faults that could affect functions protecting from safety critical events or that could propagate to flight equipment
3.A.4	Objective: System can degrade or lose functions without significantly impacting top-level expectations (through contingency operations)								
3.A.4.A	Strategy: Plan contingency or other off nominal operations	Flight Rules, FMEA, FMECA, PRA	All off-nominal conditions impacting safety or mission-success			All off-nominal conditions impacting safety			

		Evidence	Scope						
			Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
4.A	Strategy: Evaluate, control, and monitor the ease of maintaining, restoring, or changing system capability and total maintenance demands								
4.A.1	Objective: Maintenance and repair activity can be performed within available resources (cost, time)								
4.A.1.A	Strategy: Design to facilitate on-orbit and ground maintenance and check out	Design for maintainability techniques (Accessibility Analysis, Maintenance Task Analysis, Maintainability Demonstration, Process FMEA, 'Level of technician' analysis, Consumables Catalog/Limited Life Items)	Preform Maintainability Analysis consistent with the concept of Operations and Maintainability Plan					Scope the same as Class D for TRL level 3 hardware and above	Design system to support the maintenance concept and comply with Maximum downtime and availability requirements
4.A.1.B	Strategy: Design to minimize maintenance complexity for reduction of maintenance time and training requirements	Level of repair analysis, maintainability models, maintenance activities block diagrams, Maintainability Demonstration, Process FMEA 'Level of technician' analysis, Training Plan and Material Requirements for modularity/interoperability	Preform Maintainability Analysis consistent with the Concept of Operations and Maintenance Plan and design to minimize crew workload and training requirements if applicable					Scope the same as Class D for TRL level 3 hardware and above	
4.A.1.C	Strategy: During design, consider tool selection, transport, stowage, ease of use, and criticality as well as complexity of robotic maintenance capability where feasible	Level of repair analysis, maintainability models, maintenance activities block diagrams, Maintainability Design Check sheets, Process FMEA	Verify the design complies with the maintainability design requirements					Verify the design complies with maintainability design requirements (if they exist)	
4.A.1.D	Strategy: Use standardization to limit the number of feasible design options and encourage the use of common items, procedures, processes, tools, etc.	Level of repair analysis, maintainability models, maintenance activities block diagrams, Logistics/sparing analysis, Maintenance manual	Verify the design complies with the maintainability design requirements					Verify the design complies with maintainability design requirements (if they exist)	
4.A.1.E	Strategy: Perform RCM (on orbit/ground support systems) during design to optimize the design for maintainability	RCM Decision Logic Tree, RCM Analysis, Reliability Maintainability and Availability Analysis	Verify the design complies with the maintainability design requirements					Verify the design complies with maintainability design requirements (if they exist)	
4.A.1.F	Strategy: Perform maintainability simulation and analysis as needed to support design and logistic support analysis	Level of repair analysis, maintainability models, maintenance activities block diagrams, Maintainability Demonstration, RMA Analysis, Monte Carlo simulation for predicting MMH	Perform Maintainability Analysis consistent with the Maintainability Plan, Supportability Plan, and crew workload requirements if applicable					Scope the same as Class D for TRL level 3 hardware and above	
4.A.1.G	Strategy: Provide demonstration testing to verify 'detect, diagnose, isolate' capability of systems and confirm corrective and preventive maintenance task actions and analysis	Results of demonstration test which verify expected results from: testability demonstration plan, testability analysis, FMEA/CIL, Maintainability Demonstration	Test to lowest level necessary to verify Testability requirements and Mean and Maximum time to Repair Requirements					Verify the design complies with maintainability design requirements (if they exist)	

		Evidence	Scope: Human Space Flight	Class A	Class B	Class C	Class D	Research and Technology	Ground Based Systems
4.A	Strategy: Evaluate, control, and monitor the ease of maintaining, restoring, or changing system capability and total maintenance demands								
4.A.2	Objective: System provides clear indication of health status, degradations, and diagnostic information								
4.A.2.A	Strategy: Identify and optimize the testability and diagnostics characteristics to support the maintainability requirements	testability demonstration plan and results, testability analysis, MTA, I&T Reports, Ambiguity Analysis	Test to lowest level necessary to address fault detection requirements					Verify that design meets fault detection requirements (if they exist)	To Lowest level necessary to address maximum time to repair requirements and availability requirements
4.A.2.B	Strategy: Incorporate fault detection/isolation/recovery at the lowest practical level to support the maintainability requirements	testability demonstration plan and results, testability analysis, FMEA/CIL, MTA	Test to lowest level necessary to address fault detection requirements						
4.A.2.C	Strategy: Develop test-point-design strategies to minimize access time and system intrusion	testability demonstration plan and results, testability analysis, FMEA/CIL, MTA	Minimize downtime to lowest level necessary to address mean-time-to-repair requirements					Verify that design meets mean-time-to-repair requirements and false alarm rates (if they exist)	
4.A.2.D	Strategy: Design-in self-diagnostics for assemblies to minimize maintenance/recovery time and false alarms	testability demonstration plan and results, testability analysis, MTA, FMEA/CIL	Test to lowest level necessary to address mean-time-to-repair requirements and verify false alarm rates						
4.A.3	Objective: System design allows for reconfiguration, upgrade, or growth opportunities during the mission								
4.A.3.A	Strategy: Design the system to accommodate future technology or changes in application over the design life via maintenance activities	Maintenance Concept, Maintainability Design Check sheets, Recapitalization Analysis (Tech refresh), Requirements for modularity/interoperability, Material and Processes Control Plan	Verify the design complies with the maintainability design requirements	Verify system growth opportunities have been considered during System design				Scope the same as Class D for TRL level 3 hardware and above	To Lowest level necessary to address maximum time to repair requirements and availability requirements
4.A.3.B	Strategy: Design for physical and functional interchangeability with other like components and assemblies in the system	Maintenance Concept, Maintainability Design Check sheets, Requirements for modularity/interoperability, Material and Processes Control Plan, Standard Interface Requirement Document	Verify the design complies with the maintainability design requirements	Verify system growth opportunities have been considered during System design				Scope the same as Class D for TRL level 3 hardware and above	
4.A.3.C	Strategy: Incorporate modular designs to facilitate remove-and-replace maintenance and allow flexibility in the design	Maintenance Concept, Maintainability Design Check sheets, Maintainability Demo, Requirements for modularity/interoperability, Material and Processes Control Plan	Verify the design complies with the maintainability design requirements	Verify system growth opportunities have been considered during System design				Scope the same as Class D for TRL level 3 hardware and above	

		Evidence	Scope: Human Space Flight	Scope: Class A	Scope: Class B	Scope: Class C	Scope: Class D	Scope: Research and Technology	Scope: Ground Based Systems
4.A	Strategy: Evaluate, control, and monitor the ease of maintaining, restoring, or changing system capability and total maintenance demands								
4.A.4	Objective: Maintainability performance is validated and optimized during operations based on available maintenance data								
4.A.4.A	Strategy: Establish capabilities and processes to collect and store operational history, health status, degradation, diagnostic, and maintenance data	Maintainability Program Plan, Maintenance Database, FRACAS	Collect and analyze all necessary maintenance data under actual operations conditions to verify that the system's maintainability requirements are met.					Verify compliance with maintainability design requirements (if they exist)	Collect and analyze all necessary maintenance data under actual operations to verify that the system's maintainability requirements are met
4.A.4.B	Strategy: Periodically analyze test and operational history, health status, degradation, diagnostic, and maintenance data to determine maintainability performance and trends	Maintainability Program Plan, Maintenance Database, FRACAS	Collect and analyze all necessary maintenance data under actual operations conditions to verify that the system's maintainability requirements are met.					Verify compliance with maintainability design requirements (if they exist)	
4.A.4.C	Strategy: Periodically review and update maintenance strategy and activities	Maintainability Program Plan, FRACAS	Collect and analyze all necessary maintenance data under actual operations conditions to verify that the system's maintainability requirements are met.					Verify compliance with maintainability design requirements (if they exist)	
4.A.4.D	Strategy: Ensure availability of data to future programs and projects	Maintainability Program Plan, FRACAS, Lessons Learned, Insertion of data into some NASA-wide database	Collect and analyze all necessary maintenance data under actual operations conditions to verify that the system's maintainability requirements are met.					Verify compliance with maintainability design requirements (if they exist)	

APPENDIX C. R&M EVIDENTIARY METHODS

The following is a series of tables containing R&M Methods, providing brief descriptions of R&M-related analyses and activities that have proven effective on past programs. Each method is accompanied by a brief synopsis of what it does, why it is used, when it is called for, and when during a program or project it is performed.

Reliability Analysis Methods

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Alert Reporting	Document significant problem and nonconforming item data for exchange among NASA Centers and GIDEP.	To communicate across project/programs and identify potential problems.	Used throughout a program / project (extends beyond just R&M).	As close to problem identification as possible.	NASA PRACTICE NO. PT-TE-1428, "Practice of Reporting Parts, Materials, and Safety Problems (Alerts)"
Approved Parts List	Identify parts to be approved for use on a given program/project.	To restrict use of parts to those with known failure rates, lifetimes, and readily available information to help resolve problems that arise.	Commonly used on spaceflight programs/projects.	Early in design phase/process.	
Availability Analysis	Perform availability assessment that can provide quantitative performance measures that may be used in assessing a given design or to compare system alternatives to reduce life cycle costs.	To ensure maintenance resources (personnel, spare parts, test equipment, facilities, etc.), and maintenance concepts will adequately support overall system operational availability and mission success probabilities.	If operations and support costs are a major portion of the life cycle costs, or if supportability and readiness are major concerns.	During system design.	NASA PRACTICE NO. Technique AT-3, "Availability Prediction and Analysis"
Human Error Risk Assessment	Identify risks to designs, equipment, procedures, and tasks as a result of human error.	To identify candidate designs to support both risk and maintainability goals.	For both ground and manned spaceflight programs/projects.	Initially early in design and iteratively as the design matures.	

Reliability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Human Factors Task Analysis	Analyze and list all the things people will do in a system, procedure, or operation with details on: (a) information requirements; (b) evaluations and decisions that must be made; (c) task times; (d) operator actions; and (e) environmental conditions.	To identify influence factors that drive design for maintainability.	For both ground and manned spaceflight programs/projects.	Initially early in design and iteratively as the design matures.	
Deep Dielectric Charging & Internal ESD (IESD)	Conduct a materials inventory, resistivity analysis, and shielding assessment, and ascertain material susceptibility to deep dielectric charging and discharge.	To identify the potential for a charged spacecraft conductor to cause an arc/pulse which can couple into the subsystem electronics.	If the spacecraft will be subjected long-term to an energetic electron environment.	Potential IESD sources should be identified early in the program/project and eliminated.	NASA PRACTICE NO. PD-AP-1316, "Thick Dielectric Charging / Internal Electrostatic Discharge (IESD)
Failure Mode and Effects (& Criticality) Analysis (FMEA/ FMECA)	Perform a systematic, bottoms-up analysis of the local and system effects of specific failure modes of the equipment. For FMECA, also evaluate the mission criticality of each failure mode.	To evaluate fault tolerant capabilities, such as redundancy. To identify potential single point failures requiring corrective action. To identify critical items. To support a failure/anomaly triage, in the event of an anomaly.	Beneficial for all missions that have a need for some level of fault tolerance. High risk classification may require less formality, but this will help to identify highest priority allocation of limited resources.	As soon as a system block diagram is available. Update throughout system design and operations. FMECAs performed at a functional level should be developed during architectural design phase and updated as the design evolves. Piece-Part FMECAs should be developed when early candidate flight designs are available (preliminary flight schematics or drawings).	NASA PRACTICE NO. PD-AP-1307, "Failure Modes, Effects and Criticality Analysis (FMECA)"

Reliability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Fault Tree Analysis (FTA)	Systematically identify, from the top down, all possible causes of failure or an undesirable event or state (qualitatively or quantitatively).	To perform either a quantitative risk assessments or a qualitative evaluation and coverage assessment of preventions and mitigations for potential causes for system failure. Serves as a validation tool. Can be used for anomaly investigations.	It is useful for all missions that need to identify and understand potential causes for system failure. Applies to complex systems or to critical (especially safety-critical) mechanical & electromechanical hardware and include fault management controls (hardware or software).	During system design. For complex systems, FTA is performed during architecture development and refined for detailed design.	NASA PRACTICE NO. PD-AP-1312, "Team Approach to Fault-Tree Analysis"
Ground Handling Analysis	Characterize the effects on equipment of ground handling and transportation.	To identify potential problems related to handling effects, including temperature and humidity.	If functional design of spacecraft structures must consider handling effects.	Early in design.	
Limited-Life Item Analysis	Analytical and empirical engineering processes used to determine the design life.	To identify failure risks, sparing needs, or procedural requirements pertaining to equipment life of elements that have uncertain age/wear or require routine refurbishment or preventive maintenance to maintain life.	When risk or uncertainty pertaining to equipment life is a concern, such as hardware without adequate life margins.	During system design.	
Micro Meteoroid/ Debris Analysis	Predict the severity and frequency of particle collisions with a spacecraft under a specific mission profile.	To assess spacecraft vulnerability to or risk from impacts.	When the system design suggests that impacts presents a risk to safety or the mission.	Early in design.	NASA PRACTICE NO. PD-EC-1107, "Micrometeoroid Protection”

Reliability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Parts Control Plan	Describes the process used to control the pedigree of component parts of a program/project.	To provide a consistent means of identifying and controlling part lots, standardizing part selection, and controlling parts characteristics requirements.	Appropriate for all hardware programs.	Developed prior to parts selection and purchase.	
Parts Traceability	Trace parts pedigree from manufacturer to user.	In the event of failure, to provide a means to identify the source and production lot as well as to maintain consistency in parts control.	Appropriate for all hardware programs.	Early in design through disposal.	
Part Electrical Stress Analysis (PSA)	Evaluate the maximum electrical and thermal stresses on electronic parts at the anticipated part temperature experienced during the hardware qualification test to verify design margin (derating) requirements.	To reduce applied stress in order to lower component failure rates (e.g. derating); To find design flaws, such as excessive electrical or thermal stresses on electronics that could lead to premature failure; To identify risk.	For all spaceflight electronic designs because PSA is part of the basic electronics design process and is low-cost.	When a candidate flight electronics design is available, (candidate flight schematics, candidate flight parts list).	NASA Preferred Practice PD-AP-1303, "Part Electrical Stress Analysis" NASA Preferred Practice PD-ED-1201, "EEE Parts Derating"
Physics of Failure Analysis	Identify and understand the physical processes and mechanisms which cause failure.	To minimize the risk of failures by understanding the relationship between failure and driving parameters (environmental, manufacturing process, material defects).	For new product technology (e.g., electronic packaging, devices) or new usage of existing technology.	Throughout new technology development, and throughout the design and build processes.	

Reliability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Reliability Assurance Plan	Identify the activities essential in assuring reliability performance, including design, production, and product assurance activities.	To ensure that design risks are balanced against program/project constraints and objectives through a comprehensive effort calculated to contribute to system reliability over the mission life cycle.	For all programs/projects with reliability performance requirements.	During program/project planning.	
Reliability Modeling (Prediction /Allocation)	Perform prediction, allocation, and modeling tasks to identify inherent reliability characteristics.	To aid in identifying reliability drivers for a given design or evaluating the reliability of competing designs, e.g. trade studies.	For reusable or crewed systems, or where failure rates are needed for tradeoff studies, sparing analysis, risk assessment, etc.	Early in design and to support FMECA and FTA quantification.	
Reliability Tradeoff Studies	Compare all realistic alternative reliability design approaches against cost, schedule, risk, and performance impacts.	To aid in deriving the optimal set of reliability performance requirements, architectures, baselines, or designs.	Cases where design options are being considered or when design options are needed. Conducted at some level on most designs/systems.	Formulation and Implementation.	NASA Preferred Practice PD-AP-1313, "System Reliability Assessment Using Block Diagraming Methods"
Single Event Effects (SEE) Analysis	Evaluate the effects of electronics malfunctions on the system caused by transient radiation environments, and Calculate the probability of device sensitivity to high-energy particle impacts in the anticipated environment.	To prevent circuit failures caused by high-energy particle induced device upsets, latchups, gate ruptures, and transients. To mitigate SEE induced malfunctions so that the effects are tolerable in comparison to mission objectives. To identify risk.	For missions that will experience transient radiation environments with high-energy particle that can have serious consequences.	Early during design. Planning is started during electronic parts selection and detailed analysis is performed when a candidate flight design is available (flight parts list and flight schematics).	

Reliability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Sneak Circuit Analysis	Methodically identify sneak conditions (unexpected paths or logic flows) in circuits.	To identify design weaknesses that could inhibit desired functions or initiate undesired functions.	Generally used only on the most safety or mission critical equipment.	Early in design.	NASA Preferred Practice PD-AP-1314, "Sneak Circuit Analysis Guideline for Electro-Mechanical Systems"
Structural Stress Analysis	Analyze the mechanically and thermally induced loads and stress to be experienced by mechanical/electro-mechanical subsystems/assemblies, including worst-case estimates, for all anticipated environments.	To find and prevent design problems that could result in structural failure and to build-in/verify design margin. Addresses material fatigue and fracture, and the effect of thermal cycling on solder joints, conformal coating, and other critical materials.	When critical spacecraft assemblies are to be subjected to dynamic stresses or cycling environments, or when the design usage exceeds previously qualified temperature range and thermal cycling conditions.	During structural/mechanical design.	NASA Preferred Practice PD-AP-1318, "Structural Stress Analysis"
Surface Charging/ESD Analysis	Analyze differential charging of nonconductive materials on the spacecraft surface to determine whether discharges are possible.	To identify surfaces that are conceivable ESD sources and could cause unpredictable and catastrophic failures.	For any design that may be susceptible to arc discharge, such as a design that may have surfaces (conductive or non-conductive) that can build up differential charges.	Early enough in the program/project so that effects can be mitigated by grounding, coatings, RC filters, alternate materials, etc.	NASA Preferred Practice PD-AP-1301, " Surface Charging / ESD Analysis"
Thermal Analysis of Electronic Assemblies to the Part Level	Calculate the temperature of all device failure sites (i.e., junctions, windings, etc.) by estimating the thermal rise from the thermal control surface across the thermal pathways to the heat sources to verify thermal margin requirements.	To find and prevent design problems that could result in thermally induced failure (such as excessive junction temperatures) and to build-in/verify design margin.	Whenever a design contains non-negligible heat sources, temperatures and adequate heat flow should be verified. Typically performed whenever Parts Stress Analysis is required.	When a candidate flight thermal design is available (Temperature requirements defined, candidate flight board layout, candidate flight parts list, power estimates are available.) Concurrently with the Parts Stress Analysis.	NASA Preferred Practice PD-AP-1306, "Thermal Analysis of Electronic Assemblies To The Piece Part Level"

Reliability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Thermal Stress/Fatigue Analysis	Analyze thermal effects on piece parts, assemblies, and subsystems, including worst-case estimates, for all anticipated environments.	To address material fatigue and fracture, and the effect of thermal cycling on solder joints, conformal coating, and other critical materials.	When the design usage exceeds previously qualified temperature range and thermal cycling conditions.	Prior to or in conjunction with early design reviews.	
Trend Analysis	Evaluates variation in data based upon data sampled during a given timespan with the ultimate objective of forecasting future events based on examination of past results.	Before launch, to assess the status of a program/project or the maturity of a system or equipment reliability and to estimate future performance. In flight, it is performed to track the health of a system and estimate future performance.	Before launch, in cases when there is a need to assess the maturity of a system, design, or process in terms of occurrences of failures/anomalies, quality processes, delivery dates, etc. After launch, in cases when decisions are needed pertaining to life-limited (i.e., consumables) items.	Throughout the program/project lifecycle.	
Worst Case Analysis (WCA)	Evaluate performance both at a functional and a circuit level in the presence of performance limiting factors, such as part variations (associated with aging, temperature, radiation, tolerances), circuit variations (e.g. loading, timing, noise, etc.) or other relevant factors.	To ensure that equipment will perform as required over a given lifetime while experiencing the worst possible variations of electrical piece-parts and environments and to understand/verify design margin and to identify risk.	On critical flight equipment.	When a candidate flight design becomes available.	NASA Preferred Practice PD-ED-1212, "Design and Analysis of Electronic Circuits for Worst Case Environments And Part Variations"

Maintainability Analysis Methods

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Link Analysis	Arranges the physical layout of instrument panels, control panels, workstations, or work areas to meet specific objectives; e.g., increased accessibility.	To provide an assessment of the connection between (a) a person and a machine or part of a machine, (b) two persons, or (c) two parts of a machine.	During design for maintainability.	During Formulation and early Implementation.	
Logistics Support Analysis/Plan	Examine the resource elements of a proposed system to determine the required logistic support and to influence system design.	To provide an integrated and coordinated approach to meeting support requirements and attaining a maintainable design.	Where supportability and readiness are major concerns.	Early in concept development and design.	
Maintainability Modeling (Prediction / Allocation)	Perform prediction, allocation, and modeling tasks to estimate the system mean-time-to-repair requirements.	To determine the potential of a given design for meeting system maintainability performance requirements.	Whenever maintainability requirements are designated in the design specification.	Early in design.	NASA Preferred Practice Technique No. AT-2, "Mean Time to Repair Predictions"
Maintenance Concept	Describe what, how, and where preventive and corrective maintenance is to be performed.	To establish the overall approach to maintenance for meeting the operational requirements and the logistics and maintenance objectives.	Performed for ground and flight based systems where maintenance is a consideration.	During Formulation and revise throughout the life cycle.	NASA Preferred Practice Technique No. PM-3, "Maintenance Concept For Space Systems"

Maintainability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Maintenance Engineering Analysis	Describe the planned general scheme for maintenance and support of an item in the operational environment.	To provide the basis for design, layout and packaging of the system and its test equipment and establishes the scope of maintenance resources required to maintain the system.	For systems that have the ability to be maintained by preventive maintenance /refurbishment or those that allow for planned or suggested preventive maintenance operations (reversals of mechanisms, test actuations, etc). A Maintenance Plan may be substituted on smaller programs/projects where maintainability prediction and analysis are not required.	Begins during design and is iterated through development.	
Maintenance Plan	Describe in detail how the support program will be conducted to accomplish the program/project goals.	To identify the desired long-term maintenance characteristics of the system, and the steps for attaining them.	Performed for ground and flight based systems where maintenance is a consideration.	Prepare during concept development and update throughout the life of the program/project.	
Reliability Centered Maintenance (RCM)	Determines the mix of corrective, preventive, and maintenance practices to provide the required reliability at the minimum cost. Uses diagnostic tools and measurements to assess when a component is near failure and should be replaced.	To minimize or eliminate more costly, unscheduled maintenance and minimizes preventive maintenance.	Called for as part of the Maintenance concept.	During system definition throughout the lifecycle.	NASA Preferred Practice Technique No. PM-4, "Preventive Maintenance Strategies Using Reliability Centered Maintenance (RCM)"

Maintainability Analysis Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Testability Analysis	Assess the inherent fault detection and failure isolation characteristics of the equipment.	To improve maintainability in response to operational requirements for quicker response time and increased accuracy.	Where maintenance resources will be available, but constrained.	Early in design.	
Tradeoff Studies	Compare realistic alternative maintainability design approaches against cost, schedule, risk, and performance impacts.	To determine the preferred support system or maintenance approach in accordance with risk, performance, and readiness objectives.	Performed where alternate support approaches or maintenance concepts involve high-risk variables.	Complete early in the acquisition cycle.	

Reliability Test and Evaluation Methods

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Acoustics Test	Subject potentially susceptible hardware to the dominant dynamic launch environment, with adequate margin.	To qualify the design, and reveals design and workmanship inadequacies that might otherwise cause problems in flight.	For spacecraft structures with relatively large surface area-to-mass ratios, or for complete spacecraft.	At the earliest point the hardware is available for test.	NASA Preferred Practice GUIDELINE NO. PT-TE-1407, "Assembly Acoustic Tests"
Constant Acceleration Test	Subject equipment to high-G forces using a centrifuge.	To Demonstrate the ability of spacecraft structures to withstand constant acceleration/deceleration.	Where hardware is to be subjected to high-G forces, especially upon landing.	During hardware qualification.	
EMC Emissions Test	Test to identify unintentional radiated or conducted electromagnetic emissions from a system, subsystem, or assembly.	To Qualify flight hardware to launch vehicle requirements and to assure that assemblies and subsystems will be electromagnetically compatible.	For assembly, subsystem, and system level compliance testing.	Prior to hardware integration at the next level of integration.	NASA Preferred Practice GUIDELINE NO. GT-TE-2401, "EMC Guideline for Payloads, Subsystems, And Components"
EMC Isolation Test	Measure the electrical isolation between power leads and structure, and between selected signal and command leads and structure.	To verify that circuits required to be isolated from the spacecraft structure to satisfy groundings are in fact isolated.	For assembly, subsystem, and system level compliance testing.	Prior to hardware integration at the next level of integration.	

Reliability Test and Evaluation Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
EMC Susceptibility Test	Determine hardware susceptibility to electromagnetic radiation and to conducted ripple or transients on power and signal lines.	To verify immunity to power line and signal line noise at the subsystem level. To verify immunity to electromagnetic radiation environments at the subsystem and system level. To verify system hardness to the launch/boost/flight electromagnetic radiation environment, and radiated susceptibility safety margin for pyro devices.	For assembly, subsystem, and system level compliance testing.	Prior to hardware integration at the next level of integration.	NASA Preferred Practice GUIDELINE NO. GT-TE-2401, "EMC Guideline for Payloads, Subsystems, And Components"
Environmental Stress Screening (ESS) FRA	Subject parts to tests/environments that include burn-in, temperature cycling, and vibration.	To Screen out parts subject to infant mortality.	Applies chiefly to high volume production.	Prior to assembly.	
ESD Discharge Test	Use electrostatic discharges to simulate the effects of arc discharges due to space charging.	To determine electromagnetic discharge that may result in failure of circuit when such discharges occur.	Missions where the environment may produce arcing due to differential charging.	During assembly level testing.	
Ground Handling Test	Simulate the effects of ground handling and transportation dynamics.	To demonstrate the capability of equipment to withstand adverse handling conditions such as deteriorated highway roadbeds.	For critical (especially safety-critical flight) hardware (e.g., explosive devices).	During hardware qualification.	
Highly Accelerated Life Test (HALT)	Conduct synergistic thermal, dynamic, and functional (voltage, clock margining) test-to-failure on prototype or surrogate hardware.	To identify rapidly the generic design, process, or workmanship problems in advance of the hardware build.	On new hardware technology or new processes, or to verify process stability.	Prior to hardware environmental test.	

Reliability Test and Evaluation Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Highly Accelerated Stress Test (HAST)	Conduct synergistic thermal, dynamic, and functional (voltage, clock margining) accelerated stress screening.	To precipitate latent defects prior to product use.	On all high reliability flight hardware.	Prior to formal acceptance test.	
Life Testing	Perform tests under conditions expected during life to determine the useful lifespan of the article under test.	To validate estimates of assembly lifespan.	Long missions/usage or unknown components.	Pre-PDR when flight-like surrogate hardware is available.	
Magnetic Test	Measure DC magnetic fields that might be present due to materials or circuitry.	To verify that the magnetic fields created by hardware are within acceptable ranges.	Driven by science complement or attitude control requirements.	During assembly level testing.	NASA Preferred Practice PD-ED-1207, "Magnetic Design Control For Science Instruments"
Mechanical Shock Test	Simulate dynamic effects due to sources other than pyrotechnic devices.	To qualify the design for sources of shock such as pneumatic release devices and impact at the end of mechanical travel restraints.	Where mechanical shock (other than pyrotechnic) poses damage to flight equipment.	During hardware qualification.	
Powered-On Vibration Test	Continuously monitor electrical functions while power is supplied to electronic assemblies during vibration, acoustics, and pyrotechnic shock.	To detect intermittent or incipient faults (arcing, open circuits, relay chatter) in electronic circuitry that may not be observed under ambient functional testing.	For equipment where intermittent or incipient failures could compromise essential functions.	As part of a vibration test.	NASA Preferred Practice PT-TE-1405, "Powered-On Vibration"
Problem Failure Reporting (*cross listed under the Maintainability Test and Evaluation Methods*)	Provide a closed-loop system for documenting hardware, software, and procedural anomalies impact, analyzing their impact, and tracking them to their resolution.	To ensure that problems are systematically evaluated, reported, and corrected.	All programs/projects working with mission essential equipment (such as flight/flight-like equipment, support equipment, etc.) will benefit from some type of formal, closed-loop system.	Whenever flight-like designs/equipment are under development or being tested.	NASA Preferred Practice PD-ED-1250, "Pre-Flight Problem/Failure Reporting Procedures"

Reliability Test and Evaluation Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Pyrotechnic Shock Test	Simulate the dynamic effects resulting from the firing of pyrotechnic devices in spacecraft hardware, with adequate margin.	To qualify the design, and demonstrates equipment survivability in a pyroshock environment.	Where the firing of pyros may endanger flight equipment.	Simulated shock at the assembly level and live firings during system-level testing.	NASA Preferred Practice PT-TE-1408A, "Pyrotechnic Shock Testing"
Random Vibration Test	Simulate the acoustically induced vibration mechanically transmitted into hardware through attachments, with adequate margin.	To qualify the design, and assists in finding existing and potential failures in flight hardware so that they can be rectified before launch.	For qualification and acceptance of spaceflight hardware subject to acoustically induced vibration.	At the assembly level, the subsystem level and at the system level.	NASA Preferred Practice PT-TE-1413, "Random Vibration Testing"
Reliability Demonstration	Conduct tests in a nonstressed environment to verify that the equipment meets functional and reliability performance requirements.	To verify achievement of quantitative reliability and performance characteristics.	Only when expendable hardware is available, otherwise burn-in is conducted during system integration.	Following acceptance tests.	
Reliability Growth Test	Conduct repetitive test and repair cycles to disclose deficiencies and verify that corrective actions will prevent recurrence.	To ensure evolution of a system to a state of higher reliability through repeated failure and repair.	For reusable equipment.	Beginning with design and throughout the product lifecycle.	
Reliability Test Program Plan (Program/ Project Specific)	Identify and schedule tests to assess and assure reliability throughout the reliability program for a specific program/project.	To assure a thorough test program that qualifies/verifies all the hardware of a specific spacecraft.	For all programs/projects.	Formulation, and Implementation.	
Root Cause Analysis (*cross listed under the Maintainability Test and Evaluation Methods*)	Perform the analysis using deductive reasoning to identify systematic and organizational causes for the occurrence of an undesired event or anomaly.	To identify "root cause(s)" so that these latent factors may be eliminated or modified and future occurrences of similar problems or mishaps may be prevented.	Under circumstances when significant anomalies or issues occur.	During Implementation, and operations.	

Reliability Test and Evaluation Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Sine Burst Test	A method to apply static forces to simulate worst case loading conditions using a shaker.	To demonstrate hardware design load capabilities.	For assembly, subsystem and system level testing where verification for static loads has not been completed in some other manner.	During hardware qualification. Often performed when mounted on the shaker for random vibration.	NASA Preferred Practice PT-TE-1420 "Sine-Burst Load Test"
Sine Dynamic (Sinusoidal Vibration) Test	Simulate the effects of mechanically transmitted, low frequency launch vehicle transient events, with adequate margin.	To qualify the design, and reveal failure modes associated with launch vehicle transients. To qualify assemblies that will see sine vibration at higher levels of testing. Permits greater displacement excitation of the test item in the lower frequencies.	If spacecraft or assembly structure has low frequency resonances that may be excited by launch vehicle transient events.	During hardware qualification. Often performed when mounted on the shaker for random vibration.	NASA Preferred Practice PT-TE-1406 "Sinusoidal Vibration"
Structural Proof Loading Test	Apply static forces to simulate worst case loading conditions, with adequate margin.	To demonstrate hardware design load capabilities.	For primary spacecraft structures.	When either a structural test model or a flight model is available for test.	
Thermal Cycling Test	Simulate in a vacuum the effects of thermal cycling over unit life, with adequate margin.	To precipitate coefficient of thermal expansion induced fatigue related defects from design or manufacturing processes that could result in operational failure.	For all assemblies.	Prior to hardware integration at the next level of assembly.	NASA Preferred Practice PT-TE-1402, "Thermal Cycling"
Thermal Shock Test	Subject mechanical, electronic, and spacecraft structural assemblies to a high rate of temperature change in a vacuum, with adequate margin.	To qualify hardware for high ramp rates that could cause material fatigue or fracture due to thermal expansion.	For assemblies that experience wide ranges of temperature excursion with a high rate of temperature change (e.g., solar panels).	Prior to hardware integration at the next level of assembly.	

Reliability Test and Evaluation Methods (cont.)

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Thermal Test	Simulate hardware design boundary conditions of conductive and radiative heat transfer, with adequate margin.	To qualify hardware for vacuum and temperature conditions similar to the space environment. To screen for workmanship defects.	For all assemblies.	Prior to hardware integration at the next level of assembly.	NASA Preferred Practice PT-TE-1404, "Thermal Test Levels & Durations"
Voltage / Temperature Margin Test	Test the hardware under conditions that exceed the expected flight limits of voltage, temperature, and frequency to simulate hardware worst-case functional performance.	To verify functional performance over extreme conditions, to simulate EOL performance, to assess performance design margins.	A viable alternative to Worst-Case Analysis for flight programs/projects where tradeoffs of risk versus development time and cost are appropriate.	System design and integration.	NASA Preferred Practice PT-TE-1431, "Voltage & Temperature Margin Testing"

Maintainability Test and Evaluation Methods

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	IN WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Maintainability Demonstration	Conduct formal simulations of equipment repair.	To verify whether diagnostic/testability characteristics and quantitative maintainability characteristics meet system specifications.	For critical equipment where downtime must be minimized.	Prior to initial fielding of the system.	
Problem Failure Reporting *(cross listed under the Reliability Test and Evaluation Methods)*	Provide a closed-loop system for documenting hardware, software, and procedural anomalies impact, analyzing their impact, and tracking them to their resolution.	To ensure that problems are systematically evaluated, reported, and corrected.	All programs/projects working with mission essential equipment (such as flight/flight-like equipment, support equipment, etc.) will benefit from some type of formal, closed-loop system.	Whenever flight-like designs/equipment are under development or being tested.	NASA Preferred Practice PD-ED-1250, "Pre-Flight Problem/Failure Reporting Procedures"
Root Cause Analysis (*cross listed under the Reliability Test and Evaluation Methods*)	Perform the analysis using deductive reasoning to identify systematic and organizational causes for the occurrence of an undesired event or anomaly.	To identify "root cause(s)" so that these latent factors may be eliminated or modified and future occurrences of similar problems or mishaps may be prevented.	Under circumstances when significant anomalies or issues occur.	During Implementation, and operations	
Reliability Centered Maintenance (RCM)	Determines the mix of reactive, preventive, and proactive maintenance practices to provide the required reliability at the minimum cost. Uses diagnostic tools and measurements to assess when a component is near failure and should be replaced.	To minimize or eliminate more costly, unscheduled maintenance and minimizes preventive maintenance.	Called for as part of the Maintenance concept.	During Implementation.	NASA Preferred Practice Technique No. PM-4, "Preventive Maintenance Strategies Using Reliability Centered Maintenance (RCM)"

Technical Review Methods

ACTIVITY	WHAT IS DONE	WHY IT IS DONE	UNDER WHAT CIRCUMSTANCES IS IT CALLED FOR	WHEN IT IS PERFORMED	NASA Preferred Reliability Practices
Detailed Technical Reviews	Conduct formal, informal, working-level, or peer reviews to assess interface compatibility and to prevent propagation of deficiencies to later products and to assure that the proposed design and implementation approach will satisfy the system and subsystem functional requirements.	To facilitate early detection and correction of design deficiencies. To ensure that the proposed design approach, and the manufacturing and test implementation plans, will result in an acceptable product with minimal project risk.	As required to assess design compliance.	At various milestones as specified in the program/ project schedule and planning documents.	NASA Preferred Practice PD-ED-1215.4, "Common Review Methods for Engineering Products"
Launch Readiness Review	Verify readiness to launch. Review risks associated with all unresolved problems.	To determine whether to permit the launch.	For all spacecraft and payloads.	Prior to launch.	
Monitor/Control of Suppliers	Provide confidence in integrity and pedigree of supplier products and services.	To establish long-term relationships with suppliers that enhance product reliability, quality, and repeatability.	As required to control design compliance.	Formulation and early Implementation.	
Pre-Ship Review	Provide an independent assessment of product readiness for shipment.	To ensure the completeness and readiness of each item prior to release for shipment to another facility.	Where there is a need to review completion of development work before a product leaves the facility.	At the completion of the fabrication or build and testing of the item to be shipped.	NASA Preferred Practice PD-ED-1215-5, "Pre-Ship Review"
Reliability Audits	Assess the effectiveness of subsystem/subcontractor reliability assurance activities.	To identify necessary corrective actions to meet program/project R&M requirements.	Where required by the customer, or where subcontractor capabilities or the technology indicate possible problems.	Throughout design and development. Specific documentation may be required of the contractor at designated times.	
Subsystem Inheritance Review	Review the design and test requirements and failure history of inherited hardware and designs.	To identify risks associated with using inherited hardware in a new application.	When using inherited hardware.	Prior to subsystem technical reviews.	NASA Preferred Practice PD-ED-1262, "Subsystem Inheritance Review"

APPENDIX D. REFERENCES

D.1 Purpose

The purpose of this appendix is to provide guidance and is made available in the reference documents below. The following documents are considered to be useful as background information for the reader in understanding the subject matter but do not constitute requirements of the Standard.

D.1.1 Government Documents

NPR 7120.8	NASA Research and Technology Program and Project Management Requirements
NPR 7123.1	NASA Systems Engineering Processes and Requirements
NPR 8000.4	Agency Risk Management Procedural Requirements
NPR 8705.4	Risk Classification for NASA Payloads
NID 8000-108	Agency Risk Management Procedural Requirements
NASA-STD 8709.22	Safety and Mission Assurance Acronyms, Abbreviations, and Definitions
NASA-STD-8719.24	Annex NASA Expendable Launch Vehicle Payload Safety Requirements: Requirements Table
NASA/SP-2007-6105	NASA Systems Engineering Handbook
NASA/SP-2010-580	NASA System Safety Handbook, Volume 1: System Safety Framework and Concepts for Implementation
NASA/SP-2014-612	NASA System Safety Handbook, Volume 2: System Safety Concepts, Guidelines, and Implementation Examples