AEROSPACE REPORT NO.
TOR-2007(8583)-6889

Reliability Program Requirements for Space Systems

10 July 2007

Prepared by

J. B. INGRAM-COTTON,[1] M. J. HECHT,[2]
R. J. DUPHILY,[3] M. ZAMBRANA,[4] T. HIRAMOTO,[5]
C. O'CONNOR[6]
[1]Systems Engineering and Software, Corporate Chief Architect/Engineer; [2]Software Acquisition and Process Department, Software Engineering Subdivision;
[3]Acquisition and Risk Planning Office, Mission Assurance Subdivision; [4]Space and Missile Systems Center, EAS;
[5]Teledyne Brown Engineering; [6]bd Systems

Prepared for

SPACE AND MISSILE SYSTEMS CENTER
Air Force Space Command
483 N. Aviation Blvd
El Segundo, CA 90245-2808

Contract No. FA8802-04-C-0001

Systems Planning and Engineering

THE AEROSPACE CORPORATION
EL SEGUNDO, CALIFORNIA

AEROSPACE REPORT NO.
TOR-2007(8583)-6889

RELIABILITY PROGRAM REQUIREMENTS FOR SPACE SYSTEMS

Prepared by

J. B. INGRAM-COTTON,[1] M. J. HECHT,[2] R. J. DUPHILY,[3] M. ZAMBRANA,[4]
T. HIRAMOTO,[5] C. O'CONNOR[6]
[1]Systems Engineering and Software, Corporate Chief Architect/Engineer; [2]Software Acquisition and Process Department, Software Engineering Subdivision; [3]Acquisition and Risk Planning Office, Mission Assurance Subdivision; [4]Space and Missile Systems Center, EAS; [5]Teledyne Brown Engineering; [6]bd Systems

10 July 2007

Systems Planning and Engineering
THE AEROSPACE CORPORATION
El Segundo, CA 90245-4691

Prepared for

SPACE AND MISSILE SYSTEMS CENTER
Air Force Space Command
483 N. Aviation Blvd
El Segundo, CA 90245-2808

Contract No. FA8802-04-C-0001

RELIABILITY PROGRAM REQUIREMENTS FOR SPACE SYSTEMS

Prepared by:

J. B. INGRAM-COTTON
Systems Engineering and Software
Corporate Chief Architecture/Engineer

R. J. DUPHILY
Acquisition and Risk Planning Office
Mission Assurance Subdivision

Approved by:

F. L. KNIGHT, Systems Director
Systems Engineering and Software
Corporate Chief Architect/Engineer

G. A. JOHNSON-ROTH
Acquisition and Risk Planning Office
Mission Assurance Subdivision

Contents

1. SCOPE

1.1 Purpose

This document prescribes general reliability requirements for space contracts involving the design, development, (both hardware and software), fabrication, test, and/or operation of space vehicles, spacecraft bus, payloads (including those supplied as government furnished equipment (GFE)), and launch vehicles.

1.2 Applicability

The reliability requirements stated in this document are for space and launch system acquisition programs. The requirements apply to all prime, associate, and subtier contractors.

Contractors are responsible for planning and implementing a reliability program that is consistent with the program's risk tolerance posture and the contract requirements. All tasks described in this document are subject to tailoring to achieve an optimal reliability program that takes into account the programmatic and mission requirements. Examples of programmatic requirements are program resources, single-point failure strategy, make-or-buy strategy (hardware and software), on-orbit anomaly handling and resolution, downtime and restoration time requirements, and the relative importance of the program to the customer. Mission requirements include such factors as design life, mean mission duration, reliability, maintainability, availability, success criteria, program class (A, B, C, D), and derating criteria. These requirements can determine which reliability tasks may be tailored without an unacceptable increase in program risk.

The reliability tasks in this document include those tasks that generally apply to a space/launch vehicle program. Each space/launch vehicle program would include all or a subset of the tasks described in this document. The specific reliability tasks imposed on a contractor would depend upon various factors associated with each contract, e.g., mission objectives, mission criticality, budget constraints, statement of objectives (SOO), statement of work (SOW), deliverables, etc.

1.3 Approach

The contractor's reliability organization will be a major factor in the effectiveness of the implementation of the reliability requirements in this document. The contractor should have an identified reliability organization and plan. This organization should be responsible for the planning and management of the contract Reliability Program Plan (RPP) and for ensuring its effective execution. The reliability program requirements stated in this document shall require:

a. A documented and effectively planned management of the reliability effort.

b. Implementing a set of reliability program activities that are consistent with the reliability requirements and are adequate to mitigate the reliability risks to achieve mission success.

c. Involvement in the design process, performed concurrently with the evolution of the system design, to assure that reliability requirements are reflected in the final design.

d. Involvement with the software development process to assure that reliability, recovery, and diagnostics requirements are reflected in the design and carried forward into unit and integration testing.

e. Definition of the major reliability tasks and their place as an integral part of the design, development, and verification process.

f. Planning and evaluating the reliability of the system and its elements through a program of analysis, review, and test coordinated with quality assurance and all test planning functions to ensure maximum coverage of reliability requirements, availability, and recovery time requirements and to minimize repetitive or duplicative testing.

g. Timely status indication by documentation and other reporting methods to facilitate control of the reliability program.

1.4 Reliability Data Items

Appendix A, "Contractor Reliability Data Items," lists the reliability program plan and other attributes data identified in this document. This data conveys technical information to support technical decisions, to provide visibility for evaluating reliability status of the hardware, and in order to provide visibility for assessing the overall reliability program. The specific requirements for the data will be specified in the program Contract Data Requirements List (CDRL).

2. APPLICABLE DOCUMENTS

2.1 Higher Level Requirements Documents

Where applicable, the program SOO, SOW, and system specification takes precedence over the Reliability Program Requirements document formulation and implementation.

2.2 Reference Documents

The following government and industry standards and guidelines are either referenced in this document or may contain information useful in preparing reliability engineering plans and documentation. Their inclusion below is not meant to imply endorsement of their accuracy or suitability.

MIL-STD-721	Definitions of Terms for Reliability and Maintainability
MIL-STD-756	Reliability Modeling and Prediction
MIL-STD-781	Reliability Testing for Engineering Development; Qualification & Production
MIL-STD-882C	System Safety
MIL-STD-1521B Notice 2	Technical Reviews and Audits for Systems, Equipment, and Computer Program
MIL-STD-1540E	Test Requirements for Space Vehicles
MIL-STD-1629	Procedures for Performing a Failure Mode, Effects and Criticality Analysis
MIL-STD-1635	Reliability Growth Testing
MIL-HDBK-338B	Electronic Reliability Design (dated 1 October 1998)

2.3 Compliance Documents

Where applicable, the following government and industry standards contained in the Space and Missile Systems Center (SMC) Master Compliance Document Listing takes precedence over this Reliability Program Requirements document.

Aerospace Report No. TOR-2006(8583)-5235	"Parts, Materials, and Processes Control Program for Space and Launch Vehicles"
Aerospace Report No. TOR-2006(8583)-5236	"Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles"
Aerospace Report No. TOR-20046(3909)-3537 Rev. B	"Software Development Standard for Space Systems"

Aerospace Report No. TOR-2007(8583)-6414	"Technical Reviews for Systems, Equipment and Computer Software Standard"
Aerospace Report No. TOR-2005(8583)-3 Rev. A	"Systems Engineering Requirements and Products"
Aerospace Report No. TOR-2006(8546)-4603	"Data Description and Format Specification for Space Vehicle Pre-Flight Anomalies"

3. DEFINITIONS / ACRONYMS

3.1 Definitions

Accelerated Life Testing (ALT) – Deals with the two major areas of reliability— physics and statistics of failure. ALTs provide an optimal basis for the prediction of the probability of failure. This is, in effect, the essence of a probabilistic approach to physical (structural) and functional (electrical or optical) design of a component, unit or piece part.

Assembly – An integrated set of subassemblies and/or units that comprise a well-defined part of a subsystem. Examples are: liquid engine assembly, solid motor segment, electronic equipment section, antenna assembly, solar array assembly.

Component – A component is a functional unit that is viewed as an entity for purposes of analysis, design, manufacturing, software coding, testing, maintenance, configuration management, or record keeping. Examples are hydraulic actuators, batteries, electrical harnesses, and individual electronic boxes such as transmitters, receivers, or multiplexers.

Configuration Item (CI) – An item that satisfies a documented set of requirements and includes any item required for logistic support or designated for separate procurement. Configuration items consist of selected hardware or software (or combinations of both hardware and software items) that is either designated by a government contracting agency or acquiring agency to have a configuration management concern as an end item (EI), or is proposed by the contractor for development/functional end use and is designated for individual configuration management. CIs are the basic units of configuration management. They may vary widely in complexity, size, and type. CI selection separates system components into identifiable subsets for the purpose of managing further development. Changes to CIs cannot be made without change control board (CCB) approval.

Corrective Action – A documented change in the design, process, procedure, documentation, or material that has been implemented and validated to correct the cause of a failure or design deficiency.

Criticality (of a failure) – A measure of the severity of the consequence of a failure in relation to mission performance, hazards to material or personnel, provisions for redundancy, and maintenance cost.

Critical items –The hardware, software, interface, or other items (hereinafter referred to as “items”) that require special attention because of complexity, application of state-of-the-art techniques, the impact of potential failure, or anticipated reliability problems. The contractor shall ensure that all assemblies containing critical items are identified, controlled, and a process/method is in place to retain this identification throughout the manufacturing, assembly, and test processes. Critical items are any boards, boxes, subassemblies, assemblies, and structures that contain limited life, age sensitive, reliability suspect, restricted and/or prohibited parts, materials and/or processes (PMP). All mechanical and electrical piece parts used in Mission or Safety-Critical Applications shall also be included on the critical items list

Degradation – Impairment of the full ability of primary or redundant equipment to perform one or more functions.

Demonstrated Reliability – The reliability of the current configuration based upon objective evidence, i.e., data, gathered during past performance or test under specified conditions.

Derating – Derating of a part is the intentional reduction of its applied stress, with respect to its rated stress, for the purpose of providing a margin between the applied stress and the demonstrated limit of the part's capabilities. Maintaining this derating margin reduces the occurrence of stress-related failures and helps ensure the part's reliability.

Design Life – Starting at launch, design life is the desired operating time duration for the vehicle. The designers use it to size consumables (propellant, etc.) and degradeables (solar array size, batteries, etc.).

End Item – The final product when assembled or completed and ready for use.

Environmental Stress Screening (ESS) – The process of applying mechanical, electrical, and/or thermal stresses to an item for the purpose of precipitating latent part and workmanship defects to early failure.

Failure – An incident in which an item does not perform an intended function, or performs an unintended function.

Failure Analysis – The systematic examination of an item or an event, which may include software logic, electrical, telemetry, chemical, or metallurgical evaluation, to identify and analyze the modes, mechanisms, causes, and consequences of potential and real failures.

Failure Mechanism (Hardware and Software) – The process (e.g., physical, chemical, electrical, thermal, human operator/programmer) of degradation or the chain of events that results in a particular failure mode.

Failure Mode – The characteristic manner in which a failure occurs, independent of the cause of the failure. The condition or state that is the end result of one or more failure mechanisms can result in the following failure modes: short, open, fracture, excessive wear, failure to respond, incorrect result, late result, early result, crash, hang.

Failure Mode and Effects Analysis (FMEA) – Study of a system from the lowest to the highest level 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) – Study of a system starting at the lowest hardware /software level and systematically working to higher indenture levels determining the elements in which failures can occur (failure modes) and the effects of each potential failure on the system element in which it occurs, as well as affecting other system elements. The analysis shall include a study of the relative mission significance or criticality of all potential failure modes.

Failure Rate – In reliability analysis, the failure rate is typically expressed as number of failures per hour.

Failure Reporting, Analysis, & Corrective Action System (FRACAS) – A closed-loop system for recording anomalies, assessing their impact, determining the appropriate corrective action, tracking corrective action to completion, and storing the failure data for further evaluation.

Fault Tolerant Design – A system design feature in a set of failures that were defined and validated during design as being able to occur without significant adverse impacts on subsystem or system performance. The basis for addressing this includes redundancy (either physical or functional) for hardware rollback, repeat (regression testing/Monte Carlo simulations), and substitution of a default for software.

Fault Tree Analysis – A deductive system reliability analysis method that provides both qualitative and quantitative measures of the probability of failure. It estimates the probability that a top-level event will occur by systematically identifying all possible causes leading to the top event and documents the analytic process to provide a baseline for future studies of alternative designs. The basic events in a fault tree may also be moved to a checklist and used to determine which mission assurance tasks will best mitigate the risk of the top-level event.

Failure in Time (FIT) – One FIT equals one failure per billion hours.

Formal Review – A review of a project, task, or work unit designated as formal by a cognizant convening authority per the formal review criteria.

Heritage – Term refers to previously flown space qualified hardware and software being proposed for use in new systems.

Informal Review – A review of a project, task, or work unit not designated as formal by a cognizant convening authority per the formal review criteria.

Integrated System – The integrated system consists of the entire assemblage of space vehicle, transfer vehicle (if there is one), and launch vehicle that are all launched together at the same time.

Item – Hardware or software that is incorporated into either the integrated system, module, subsystem, assembly, section, unit, subassembly, component, and/or part level (depending on which level of the hierarchy an item is used).

Inherent Reliability – A measure of reliability that excludes effects other than those proceeding from the item's design and the application of the design within an ideal operating and support environment.

Legacy – Term referring to out-of-date hardware or software still in use (see Heritage).

Material – A metallic or nonmetallic element, alloy, mixture, or compound used in a manufacturing operation that becomes either a permanent portion of a manufactured item or can leave a remnant, residue, coating, or other material that becomes or affects a permanent portion of a manufactured item.

Mean Mission Duration (MMD) – The average time an on-orbit space system is operational before a mission critical failure occurs. The MMD is the area under the reliability versus time curve truncated at the design life.

$$\text{Mean Mission Duration} = \int_{t=0}^{T} R(t)\, dt$$

where R (t) = Mission reliability model function and T = Time at truncation.

Mission Critical – 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. For non-repairable systems, an item or function where its failure will result in loss of the mission.

Mission Profile – A time-phased description of the occurrence of events within each environmental envelope that an item experiences from initiation to completion of a specified mission, that includes the criteria of mission success or critical failures at each phase. Mission profiles are used in establishing general performance requirements and are essential to evaluating reliability performance.

Module – A level of assembly made up of large structural sections and/or functional assemblies that together form one of the major elements of a larger functional system. Modules consist of related subsystems, sections, and units that together form a single structural and functional entity usually manufactured separately from the system. Modules are viewed as physical and functional entities for the purposes of analysis, manufacturing, testing, or record-keeping. Examples include a large payload portion separated from a spacecraft or bus that together with the spacecraft forms a space vehicle or satellite, or an individual stage of a launch vehicle system.

Part – A part is a single piece, or two or more joined pieces, that are not normally subject to disassembly without destruction or impairment of the design use. A part is the lowest level of separately identifiable items (e.g., piece parts).

Part Stress – Mechanical, electromagnetic, chemical, electrical, and other environmental conditions affecting the performance of electrical parts. Significant changes in piece part performance may be induced by the following factors, listed in their approximate order of significance-- temperature, aging (powered life), radiation, mechanical forces (e.g., vibration, shock, acceleration, spin), humidity, life (unpowered shelf life), vacuum, and electrical stress.

Parts Stress Analysis (PSA) – An analysis conducted to verify that the applied stress experienced by an electronic or electromechanical piece part does not exceed the stress derating values. See Derating. (Also refer to Aerospace Report No. TOR-2006(8583)-5235, *Parts, Materials, and Processes Control Program for Space and Launch Vehicles.*

Performance – A measure of how well a system or item functions in the expected environments.

Process Failure Modes and Effects Analysis (Process FMEA) – An analysis of an operation/process to identify the kinds of errors humans could make in carrying out the task. A method to deduce the consequences of process failure and the probabilities of those consequences occurring.

Reliability – The probability that an item will perform its intended function for a specified time interval under stated conditions.

Reliability Assurance – The management and technical integration of the reliability activities essential in maintaining reliable performance, including design, production, and product assurance activities. The reliability assurance function encompasses reliability engineering, as well as aspects of non-engineering activities such as procurement.

Reliability Audit – A survey of the reliability assurance activities of a subsystem group or a subtier contractor conducted to assess the effectiveness of these activities and the extent of compliance with reliability requirements.

Reliability Prediction – A forecast of the reliability of a system or system element. Reliability predictions are quantitative values that are usually calculated at an early design stage when little directly applicable test data are available.

Risk Management – An organized and coordinated means of a controlling process to identify, assess, and control/mitigate the risk on a program or project.

Section – A level of assembly made up of structurally integrated sets of hardware assemblies and interconnecting hardware that may be joined with other sections in order to form a more extensive structural or functional subsystem, module, or system configuration. Examples include solid rocket motor sections, liquid rocket engines, or large solar array sections. Sections may also include collections of electronic units mounted into a structural mounting tray or panel-like assembly.

Segment – A major product, service, or facility of the system (e.g., the space segment or ground segment).

Single Point Failure – A system failure mode that can be induced by a physical failure mechanism in a single piece-part, an interconnection, a single multilayer board, or a mechanical gear train. Includes the sense of *subassembly* as defined in DOD-STD-100, MIL-STD-280, MIL-STD-1540C, and MIL-STD-1833.

Subsystem – An assembly level consisting of two or more units and may include interconnection items such as cables or tubing, and the supporting infrastructure to which they are mounted. A subsystem is composed of functionally related units. An integrated set of assemblies that perform a clearly separated function (e.g., attitude control subsystem) involving similar technical skills. Includes the sense of group, set, and system in DOD-STD-100, MIL-STD-280, MIL-STD-1540C, and MIL-STD-1833

Support Equipment – Equipment used in the check-out and/or preparation of the flight hardware during testing, handling, verification, or pre-launch operations.

Tailoring – The process by which sections, paragraphs, and sentences of specifications, standards, and other requirements and tasking documents are evaluated to determine the extent to which they are applicable to a specific acquisition contract (or in-house development) and then modified to balance performance, cost, schedule, and risk.

Unit – Interchangeable with Component.

Worst Case Analysis (WCA) – An analysis used for determining whether a system or individual equipment item will meet all applicable specified performance requirements while being subjected to the most adverse combination of operating and environment conditions.

3.2 Acronyms

ALT	Accelerated Life Testing
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CI	Configuration Item
CIL	Critical Item List
CLSI	Custom Large Scale Integration
CSCI	Computer Software Configuration Item
DBMS	Data Base Management or Monitoring System/Subsystem
DCA	Design Concern Analysis
DoD	Department Of Defense
DRD	Data Requirement Description
EEEE	Electrical, Electronic, Electro-Optical, and Electromechanical
EMC	Electromagnetic Compatibility
EPROM	Erasable Programmable Read Only Memory
ESS	Environmental Stress Screening
FCA	Functional Configuration Audit
FIT	Failure in Time
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FPGA	Field Programmable Gate Array
FQR	Formal Qualification Review
FRACAS	Failure Reporting and Corrective Action System
FRB	Failure Review Board
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
HSIA	Hardware-Software Interaction Analysis
HWCI	Hardware Configuration Item
LRU	Line Replaceable Unit
LV	Launch Vehicle
MMD	Mean Mission Duration
MTBF	Mean-Time-Between-Failures
MTTF	Mean-Time-to-Failure
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PMP	Parts, Materials and Processes
PRR	Production Readiness Review
PSA	Parts Stress Analysis
PWB	Printed Wiring Board
RBD	Reliability Block Diagram
RPP	Reliability Program Plan
SCA	Sneak Circuit Analysis
SDR	System Design Review

SE	Support Equipment
SEE	Single Event Effect
SEU	Single Event Upset
SMC	Space and Missile Systems Center
SMQI	Space Mission Qualified Item
SOO	Statement of Objectives
SOW	Statement of Work
SPF	Single Point Failure
SPFM	Single Point Failure Mode
SRR	Systems Requirements Review
SV	Space Vehicle
TOR	Technical Operating Report
TRR	Test Requirements Review
USAF	United States Air Force
VHSIC	Very High Speed Integrated Circuits
VLSIC	Very Large Scale Integrated Circuits
WCA	Worst Case Analysis

4. GENERAL REQUIREMENTS

4.1 Reliability Program

The contractor and subcontractors shall implement and maintain a reliability hardware/software program that is planned, scheduled, integrated, and developed in conjunction with other design, development, and production functions in accordance with the contractual statement of work, the requirements of this TOR, and the program plan approved by the acquisition procurement agency. The contractor shall establish and maintain an internal system of directives, procedures, instructions, specifications, and manuals to implement the contractually required reliability program. The program level of effort shall be adequate to fulfill the contractual quantitative and qualitative reliability requirements and to support economical achievement of overall program objectives.

The tasks and requirements apply to both the hardware and software design.

4.1.1 Reliability and Related Requirements Allocations

1. Quantitative vehicle contractual reliability requirements shall be allocated to the subsystems, software, components, or piece parts, to the extent necessary to specify an allocated reliability value for a configured item specification, and to verify compliance with reliability and related requirements at the system level for such items.

2. The contractor shall document in the reliability plan the methods, models, ground rules, assumptions, limitations, and proposed verification methodology(s) for reliability and related requirements allocation.

4.1.2 Heritage Hardware and Software.

For space qualified heritage hardware and software, parameters used in the model and analyses shall be consistent with operational history data or other previously accepted values. In cases where such values are not sufficient to meet allocated requirements, revised allocations and analyses shall be performed where the off-the-shelf hardware requires modification to satisfy the reliability specification requirements.

4.2 Quantitative Requirements

The minimum acceptable item reliability shall be as stated in the configuration item specification. Quantitative reliability requirements for all major items shall be stated in the appropriate section of each specification. The quantitative values *not* defined by the system specification and those to be allocated from the systems requirements shall be established by the contractor.

4.3 Integration with Other Requirements

The reliability program effort shall be closely coordinated with the systems engineering, design engineering, and test programs as well as configuration management and integrated logistics support functions. The reliability program shall also be closely integrated with the related engineering disciplines and technical specialties of quality assurance (hardware and software), maintainability (hardware and software), human engineering, system safety, software development, and parts, materials, and processes control to preclude duplication of effort and produce integrated cost-effective results.

5. DETAILED REQUIREMENTS

5.1 Reliability Program Management, Surveillance, and Control

5.1.1 Reliability Program Overview

1. The contractor shall manage, monitor, and control all program activities associated with the reliability program and establish a system to monitor the reliability program, and status reliability tasks including, but not limited to:

    a. Establishing the control of reliability program schedules, monitoring, and control of subcontractors and suppliers

    b. Implementing and maintaining a closed-loop failure reporting and corrective action system

    c. Participating in the decision processes of the Engineering Review Board (ERB), Change Control Board (CCB), Material Review Board (MRB), and Failure Review Board (FRB)

    d. Identifying and reducing or eliminating program risks associated with system elements that have a significant impact on reliability

2. The contractor shall demonstrate reliability engineering skills to perform specific reliability engineering and evaluation tasks. These tasks shall include:

    a. Creating a reliability analysis to determine if the contractual quantitative reliability requirement and reliability-related attribute requirements have been achieved within the baseline design

    b. Allocating the system reliability requirement to lower levels of indenture for configured item specifications and establishing baseline requirements for designers and subcontractors

    c. Analyzing failure modes, effects, and criticality in order to identify single point failures and reliability improvements in a timely manner and fostering interchange of design information with other program activities (e.g., system safety, instrumentation, test, and other reliability analyses)

    d. Verifying that the actual electrical stresses comply with the approved parts derating criteria and the mechanical stresses have a positive margin of safety; verifying with PM&P any items outside the parts stress ratings category

    e. Identifying, evaluating, and controlling those critical items that require special attention because of complexity, application of state-of-the-art techniques, anticipated reliability problems, new technology insertion considerations, or the impact of potential failure on safety, readiness, and/or mission success. Preparing and maintaining a critical items list

    f. Determining the effects of storage, handling, packaging, transportation, maintenance, and repeated exposure to functional testing on hardware reliability

g. Providing reliability data on previously flown hardware to ensure its reliability and suitability for a mission. The product must meet pre-set reliability requirements as outlined within the reliability program plan

h. Identifying and evaluating critical items to justify their capability to survive the mission duration

i. Performing reliability trade studies in support of decisions on design alternatives, reliability improvements, supplier/subcontractor selections, and component/part evaluations

j. Evaluating the production operation to assure the hardware is manufactured in a repeatable and verifiable manner

k. Performing a reliability assurance function in which the reliability organization will monitor and coordinate with the appropriate technical specialists within the other analysis groups to assure that reliability-related engineering tasks are performed per the planned methodology and procedures

l. Performing a technical review of the design and analysis results from other engineering groups to identify design weaknesses and to implement a corrective action to preclude failure or degraded performance during the useful life of the system

m. Ensuring subcontractor and supplier data (e.g., reliability predictions, FMECAs, problem and failure reports, task status, analyses) are compatible with and incorporated into the overall program database

3. The contractor is responsible for performing testing and reliability verification tasks as an integral part of the independent integration, test, and verification process. These tasks shall include direct reliability involvement in new technology qualification and acceptance testing, environmental stress screening tests, accelerated life testing (ALT), developmental tests, and reliability life tests.

5.1.2 Reliability Program

The contractor shall provide, maintain, and implement a reliability program plan that complies with the reliability program requirements of this standard. It shall cover all phases of the program as it applies to reliability. The program shall ensure the management, surveillance, and control for the reliability program tasks. The contractor shall document the reliability program in accordance with the customer deliverable instructions.

The reliability program shall include:

a. A description of the contractor's reliability organization. This organizational description shall include the interface between the reliability organization and the responsibilities of each program discipline necessary to accomplish the reliability tasks

b. Narrative descriptions, schedules, and supporting documents, which describe in detail the contractor's plan for execution, implementation, and management of each task in all phases of the reliability program. All program reliability requirements shall be covered

in the reliability program task descriptions, e.g., interfaces to other disciplines, critical Item list procedures, and design guidelines, and required data

c. Contractor directives, methods, and procedures that will be used in the implementation of the reliability tasks. Existing contractor documents shall be modified, as required, to comply with the reliability requirements

d. Identification of hardware and software to be procured from subcontractors and/or suppliers, including flow-down of reliability requirements as specified in the subcontract or purchase order for each such hardware and software item

e. The reliability program requirements to be specified in the subcontract or purchase order for each such hardware and software item.

f. Identification of previously flown or heritage/legacy hardware and software to be used in the design

g. Identification of GFE to be used in the design

h. Monitoring progress and notifying the customer to provide visibility into the work performed and to highlight any significant reliability problem(s), finding(s), and contribution(s)

5.1.3 Monitoring and Control of Subcontractors and Suppliers

1. The contractor shall monitor and control supplier/subcontractor progress in meeting reliability program milestones and schedules and shall take timely action on and notify the customer of any reliability, technical, or programmatic problems when warranted.

2. The contractor shall prepare a coordinated supplier/subcontractor management, surveillance, and control program. This program shall describe the contractor's plan to manage and control the supplier/subcontractors. This program shall include but not be limited to:

   a. A list of all suppliers/subcontractors involved in the program

   b. The overall schedule for the surveillance and control of suppliers/subcontractors

   c. A schedule of major reviews to be held by the subcontractors and suppliers

   d. The reliability tasks required of the suppliers/subcontractors

   e. Attendance at supplier/subcontractor design reviews/audits

3. Direct involvement by the contractor's reliability group in the supplier selection process. The contractor shall define the major reliability factors to be used in the selection process.

4. The supplier/subcontractor shall notify the contractor of reliability problems and the contractor shall include these problems in his notification to the customer of all major reliability problems throughout all program phases, including the proposed corrective action(s).

5.1.4 Program Reviews and Audits

1. The contractor's reliability organization shall provide support to the design reviews, configuration audits, and internal design reviews/audits including subsystem and component configuration requirements.

5.1.5 Failure Reporting, Analysis, and Corrective Action System (FRACAS)

1. The contractor shall establish and implement a closed-loop system for recording and analyzing anomalies, determining the root cause, appropriate corrective action, tracking action to closure, and reporting on status of failures or anomalies. The FRACAS shall be an organized system to ensure that flight hardware and software problems, and failures detected throughout the project life cycle, are recorded and receive management attention; the root cause(s) of failures are determined; the appropriate corrective action is identified, approved, and taken; and the risk of recurrence is minimized. The contractor shall be the focal point for the program FRACAS and flow-down the FRACAS requirement to all supplier/subcontractors who are involved in the design, test, production, or operations of the program. The contractor shall ensure the subcontractor/supplier provides recurring feedback regarding the status and changes to their FRACAS.

2. The FRACAS database will meet the intent of Aerospace Report No. TOR-2006 (8546)-4603, *Data Description and Format Specification for Space Vehicle Pre-Flight Anomalies,* dated 31 January 2006.

5.1.6 Failure Review Board (FRB)

1. The contractor shall implement a formal board charged with review of hardware and software problem and test failure reports and associated trend data; investigation of incidences, root causes, and supporting documentation; assessment of the risk to the project; recommendation of the appropriate corrective actions; evaluation of the results of corrective action implementation; recommendation of FRACAS reports for closure; and the status of FRB efforts to management.

2. The contractor shall provide the government customer what his basis is for an FRB and the outputs from conducting a FRB, i.e., scope, objectives, authority, responsibilities, membership criteria, and procedures, for acceptance and approval. The contractor shall document his FRB basis in accordance with customer deliverable instructions.

5.1.7 Use of Previously Flown or Heritage Hardware and Software

The contractor shall provide evidence that proposed previously flown or heritage hardware and software will comply with allocated reliability, derating, and related performance requirements of this standard.

5.1.8 Reliability of Government Furnished Equipment (GFE)

GFE reliability analyses shall be provided by the U.S. Government. The system reliability prediction shall be performed inclusive of GFE reliability. (Note: No flight GFE will be flown without its reliability data being provided and the data's integrity evaluated).

5.2 Reliability Engineering and Evaluation

The contractor shall perform reliability predictions, failure modes effects, and criticality analysis (FMECA) and interface with trade studies, EEE parts quality/derating, worst case analysis, parts stress analysis, and hardware/software interaction analysis (HSIA) tasks as an integral part of the reliability program. These tasks shall be used to identify/manage reliability drivers, single point failures, and critical items to improve the reliability of space vehicles (SV) and launch vehicles (LV).

5.2.1 Reliability Predictions

1. The contractor shall create reliability models reflecting the design to perform reliability predictions and predict related attributes (maintainability, availability, service continuity) in conjunction with the design to assess and show compliance with numeric reliability requirements and to support allocation. The predictions shall include both hardware and software items, and the models shall include both hardware and software components.

2. The contractor shall provide all of the inputs used to perform the reliability predictions. These inputs shall include at a minimum:
   a. A complete detailed description of the model(s), data, and related information.
      (1) Nomenclature of items used in reliability block diagrams shall be consistent with that used in functional architectural diagrams, block diagrams, drawings, software documentation, schematics, weight statements, power budgets, and specifications
      (2) Be developed to the unit level and runtime software task (process) levels as a minimum, and shall include probability of success with associated failure rates. The models shall address non-recoverable and recoverable failures originating in hardware, software/firmware, communications channels, and external interfaces
      (3) Shall enable evaluation of the effects redundancy, cross-strapping, duty cycling, active versus standby hardware, critical versus non-critical hardware, and mission life limiting components
         a) Include all relevant parameters as well as the sources from which they are derived
      (4) Shall be documented, as necessary to explain the composition, construction, intent, limitations, approximations, and definition of all parameters
      (5) Describe input data. The description of input data shall identify all model parameters including failure rates, recovery times, recovery probabilities, correlated failure rates, and other parameters. Any adjustment of the parameters and the reference or other justification, shall be provided
         a) Where parameters are derived from test or operational data, the contractor shall describe the methods for parameter estimation and provide confidence limits
         b) Where parameters are expected to change due to reliability/availability growth, the contractor shall provide a complete description of reliability models, parameter estimation techniques and justification for selection of those techniques.
         c) All ground rules and assumptions used in the model(s) and prediction shall be described
   b. The model(s) shall include both the reliability block diagrams and mathematical models.

      - The reliability block diagram (RBD) and mathematical model shall include all redundancy, special success conditions, cross strapping, duty cycling, active versus standby hardware, critical versus non-critical hardware, mission time-line functions, reliability parameters (e.g., failure rates and mission time, and the success criteria)

- The RBD and mathematical model shall be organized by subsystem. The RBD and mathematical model shall include the failure rate of components and mechanical parts that compose the subsystems
- The mathematical model shall include mechanical items, as well as electrical components. The mathematical model shall be associated with the RBD
- Contractor shall have the model and the basis/assumptions used to develop and use the model substantiated by an independent validation agency
- The mathematical model shall be described to explain the model for both standard probability expressions and special models. Examples of special models include Monte Carlo simulation, Markov analyses, Weibull analyses, Bayesian models, truth tables, EEE part models, etc. The description shall include the definition of all parameters. Any mathematical model can be used as long as it is defined and described

c. The component failure rates. The derivation of the component (unit, black box) failure rates in time (FITs) and the source of the EEE part failure rates, whether dormant or active, shall be provided. These failure rates shall be shown on the RBD.

- The failure rates shall clearly show and document all adjustment factors, such as the environment, quality level, temperature, stress, and duty cycling. An explanation shall be provided for these adjustments factors
- The contractor shall provide the detail failure rate analysis on those components and/or parts for which a special failure rate analysis was performed (e.g., a failure rate computed from test or flight data)

d. Heritage hardware and software. The reliability analysis requirements of this TOR apply to heritage hardware and software. Previous analyses shall be reviewed in regard to the specific program reliability specification requirements. Those areas found deficient shall be updated to the reliability specification requirements and new analyses shall be performed where the off-the-shelf hardware requires modification to satisfy the reliability specification requirements.

3. Reliability predictions shall be used to support configuration trade studies, hardware procurement, and hardware reliability evaluations.

4. The contractor shall present sufficient reliability data and justification to support any requested changes to the system reliability prediction requirement.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

5.2.2 Failure Modes, Effects, and Criticality Analysis (FMECA)

1. The contractor shall perform a Failure Modes and Effects Analysis (FMEA)/Failure Modes, Effects, and Criticality Analysis (FMECA) on all flight hardware and software and on support equipment (SE) interfaces to the flight hardware and software.

2. The FMEA/FMECA shall:

    a. Analyze all credible failure modes of the hardware and software

    b. Describe the failure effects at the local, next higher level, and end effect levels. The local level is the level at which the analysis is performed

    c. Identify method of failure detection and associated telemetry data (other annunciation mechanisms)

    d. Describe any compensating provision that either mitigates the risk of an adverse failure effect from occurring or the consequences of an adverse failure effect that occurs

    e. Identify the criticality (i.e., severity) category

3. At any level where the FMECA is performed, the analysis shall cover failure mode categories including, but not limited to:

    a. "Hard" or permanent failures of electrical, electronic, and electromechanical (EEE) parts, including short circuits, open circuits, and incorrect function (e.g., single event effects)

    b. For software: "crash" or "fail stop" events

    c. For both hardware and software: premature operation and/or output

    d. For both hardware and software: failure to operate at prescribed time

    e. For both hardware and software: failure to cease operation at prescribed time

    f. For software: late response

    g. For software: hang or no response (while maintaining operations)

    h. For software: timely but incorrect response

4. For redundant systems, the primary objective of the FMECA shall be the identification of all credible single point failures (SPFs) that are present in the system design. These SPFs shall be included on the Critical Items List (CIL) for appropriate corrective action and risk management activities (see section 5.2.5 Critical Items).

    a. The FMECA shall identify effects upon the system resulting from redundancy management (implemented in either hardware or software). Common cause/common mode failures, interfaces, and isolation techniques for redundant elements (either hardware or software), as well as failures in the redundancy management measures themselves shall be analyzed to ensure that the desired redundancy is not negated.

5. For both redundant and non-redundant systems, the FMECA shall identify all catastrophic and critical failures that cannot be eliminated from the system. These failures shall be included in the CIL for appropriate attention in corrective and risk management activities (see section 5.2.5 Critical Items). Detail mitigating provision(s) shall be provided for the catastrophic and critical failures.

6. The FMECA shall include a functional analysis at the system and unit levels. The analysis shall include a FMECA for areas of the hardware and software (including interfaces) that are potential single point failures.

   a. Functional FMECA. The contractor shall perform a functional FMECA, including both time-dependent and time-independent failure modes. The functional FMECA normally is used when hardware items or software items cannot be uniquely identified, or when system complexity requires analysis from the initial indenture level downward through succeeding indenture levels. All system functions, including electrical, electronic, mechanical, structural, chemical, ordnance, command, telemetry, and software shall be identified in addition to the redundancy contained in each. The contractor shall develop a functional diagram of the system or applicable portions, traceable to the corresponding equipment. The contractor shall, by search, analysis, or simulation, determine the effects on system functions of single failures in accordance with the requirements of this standard. The analysis shall include the response of the system to failures where the ability to restore full system function or preserve partial system function by the use of redundancy or by other action may depend upon the elapsed time since the failure. Examples of these kinds of failures include those that lead to control instability, cyclic, thermal, or mechanical stress, or leakage of propellants. The functional FMECA shall make provision for different levels of analysis based on the mission phase and function criticality for which the function is being analyzed.

   b. Hardware/Software FMECA. As the design progresses, the contractor shall perform a more detailed FMECA, based on the physical designs of the system, subsystems, units being analyzed, and runtime software architecture (i.e., the software tasks or processes existing at runtime, their communications methods, resources, data, and underlying services). The analysis shall be performed down to the hardware level and software task or process level in the priority established by the criticality classification of the mission functions. Substantiation shall be provided for all failure rates incorporated into the critical analysis (CA). A unit FMECA shall be performed on each unit regardless of whether or not the unit or its function is redundant in the system. For redundant components, the FMECA shall be performed to provide sufficient depth to identify failure modes that can influence redundancy implementation.

   c. Interface FMECA. The contractor shall identify and analyze all of the interfaces at all levels of hardware and software. The contractor shall develop functional, block diagrams of the system incorporating both hardware and software traceable to the corresponding system elements. Failures in any one subsystem unit or interconnecting circuit which cause thermal, electrical, mechanical damage or degradation, deadlock or capacity (memory or processor throughput) due to shared resource contention, data corruption, or other types of cross-interface degradation to any other subsystem or unit, or within the unit, shall be identified. Any interfaces between the space vehicle and payloads shall be included. The analysis shall include software interfaces that can have an impact on mission success. Pin-fault analysis shall be conducted as part of this FMECA.

   d. Hardware-Software Interaction Analysis (HSIA) shall be performed to ensure software is designed to react to hardware failures in an acceptable way. It shall be performed concurrently with all hardware FMEA's involving software.

7. The FMECA shall include, at a minimum, all electronic units, major structural items, electro-mechanical items, deployment devices, propulsion items, run-time software components, and sensors.

    a. Large Scale Integration. Very Large Scale Integrated Circuits (VLSIC), Very High Speed Integrated Circuits (VHSIC), Custom Large Scale Integration (CLSI), and Hybrid Semiconductor Devices shall be analyzed for all failure modes external to these devices, including, but not limited to, failed open or closed, out of sequence, and out of time window signals at each electrical contact ("pin"). If such devices included firmware, firmware failures shall be included in the analysis. Where electrical contacts are equivalent, the analyses may be aggregated. Hardware/Software FMECAs (paragraph 6a above) and product design –manufacturing FMECAs (MIL-Std-1543, paragraph 204.2.8.4) shall be performed on these devices. Early emphasis, at or prior to PDR, shall be placed on hybrids, on new technology devices designed or modified for the system (e.g., Field Programmable Gate Arrays [FPGAs]), and on devices with no history of successful use in similar applications.

8. The FMECA shall analyze the Safe Mode design in all applicable subsystems.

9. The FMECA shall be performed on all support equipment (SE) interfacing directly with flight hardware and software. These FMECAs shall be performed on the SE interfaces with the flight hardware and software.

10. The FMECA shall be of sufficient detail and accuracy to enable the following uses:

    a. Determine the need for redundancy, fail-safe design features, and/or further derating

    b. Support systems safety analyses and hazard analyses

    c. Support establishment of safety requirements in testing and operations

    d. Ensure that the test program is responsive to known and suspected potential failure modes

    e. Establish data recording requirements and needed frequency of monitoring in testing, checkout, and mission use

    f. Support mission operations activities such as designing fault isolation sequences and alternate mode of operation planning

    g. Support establishment of quality assurance requirements in determining mandatory inspection points for critical items during manufacturing and at hardware acceptance

11. FMECAs and other analyses interfacing with them shall be coordinated closely to provide consistency and to minimize duplication. The FMECAs shall be prepared and distributed within the contractor's organization in time for the decisions and uses they are intended to support.

12. Sneak Circuit Analysis (SCA):

    a. The contractor shall assess the necessity for conducting sneak circuit analyses on an exceptional basis, i.e., when warranted by a FMECA or WCA. In the event an SCA may be warranted, the contractor will perform sufficient analyses on safety-related critical items, items that do not "fail-safe," and on new or modified safety critical designs in support of the FMECA. The analyses shall be "sufficient" in so far as to identify any latent electrical paths that may cause the occurrence of unwanted functions or inhibition of desired functions. These analyses shall be performed on design areas that are potential single point failures that have a safety critical impact, and to locate unresolved problems that could not be found by other analyses or tests. Non-modified heritage components and subassemblies shall be reviewed for sneak paths in conjunction with flight history.

    b. The contractor shall review the electrical design on the aforementioned to the extent of identifying and resolving undesirable sneak conditions. Examples of potential sneak conditions resulting in a credible safety-critical SPF include: a) a sneak path that causes current to flow along an unexpected circuit or within an IC, b) a sneak timing condition that causes or prevents the activation or inhibition of a critical function at an unexpected time, c) a sneak indication that may cause an ambiguous or false display of system operating conditions, d) a sneak label that may cause operator error through inappropriate control activation.

    c. The contractor shall obtain design and test information on exceptional items (e.g., new technology assemblies and parts that are critical items) to identify and resolve any potential sneak conditions. This information shall be obtained directly from the vendors of the new technology assemblies and parts. The information shall include all applicable design analyses, test reports and manufacturing reports.

13. Single Point Failure (SPF)

    A single point failure is any single hardware failure or software error, which results in irreversible degradation of item mission performance below contractually specified levels. The way or manner in which a single point failure of an item occurs is the single point failure mode (SPFM) of the item.

The major thrust of the FMECA and other FMECA-related analyses (e.g., sneak circuit analysis, product design FMECA, etc.) shall be identification and elimination of, or compensation for, single point failure modes to improve reliability. Emphasis shall be placed on eliminating credible Single Point Failure Modes (SPFMs) by design, or where elimination is not feasible, on reducing the SPFM likelihood or impact by incorporating compensating features. All credible SPFMs that are not eliminated by design shall be placed on the Critical Items List (CIL). The controls and/or compensating features that minimize the probability of failure of the SPFMs shall be identified and included with the CIL.

Redundancy cross-straps shall be analyzed as a potential SPF. A short-to-ground in the cross-strap design, that can fail all units tied to the cross-strap, is a SPFM.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

5.2.3 Parts, Materials, and Processes (PMP) Program Interface

1. The reliability group shall provide a check-and-balance function on the parts used in the design. This effort shall be accomplished by ensuring that the parts selected by PMP meet reliability requirements. In this regard, the reliability group shall specify requirements on part quality and/or additional screening necessary to support the satisfaction of the reliability prediction requirement. The reliability group shall also identify parts that do not satisfy the derating criteria, support PMP on any special part tests (e.g., test sample sizes, pass/fail criteria, etc.), and support the evaluation of special mechanisms for deployment and backup functions.

2. Materials and processes shall be selected on the basis of suitability for their uses as determined by past performance, available data, or current tests. Reliability shall support the selection and verification process by performing any reliability analysis of past orbital performance data and/or test data.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

5.2.4 Critical Items

The contractor shall ensure that critical items (CIs) are identified. The CIs shall be retained throughout the manufacturing, assembly, and test processes. CI examples are: boards, boxes, subassemblies, assemblies, and structures that contain limited life, age sensitive, reliability suspect, restricted and/or prohibited parts, materials and/or processes (PMP), credible single point failures that cannot be eliminated from the system, electrical, electronic, and electromechanical (EEE) items whose stress level exceeds the derating guideline of the contract, and structural and mechanical items that have a negative margin of safety.

The following are typical circumstances that would cause an item to be included on a critical items list:

- Failure of the item would lead directly to severe injury or loss of human life

- A failure of the item would seriously affect system operation or cause the system to not achieve mission objectives or meet system performance requirements for accuracy, availability, integrity, or continuity, or would represent a single point failure (i.e., any single hardware failure or software error that results in irreversible degradation of an item's mission performance below contractually specified levels—the way or manner in which a single point failure of an item occurs is the single point failure mode, or SPFM, of the item).

- A failure of the item would prevent obtaining data necessary to evaluate accomplishment of mission objectives

- The item has exhibited an unsatisfactory operating history relative to required performance or reliability

- The state-of-art item has inadequate data in its intended application to assess its acceleration factor

- The selected item does not have sufficient history or similarity data to compare with other items that have demonstrated high reliability
- State-of-the-art techniques are required to manufacture the item
- The items are stressed in excess of derating criteria
- The item has an operating, shelf-life, or environmental exposure limitation that warrants controlled storage or use
- The item is known to require special processing, handling, transportation, storage, or test precautions
- The item's past history, nature, function, or processing warrants total traceability

Any item accepted by waiver or deviation becomes a critical item.

For each item on the CIL, the contractor will identify the compensating features in the design, control methods, procedures or risk mitigation plan to be incorporated to minimize the occurrence of a failure associated with the critical item.

5.2.5 Reliability Support to Trade Analyses

1. The contractor shall consider reliability in trade studies that involve: a) program design trade studies, b) reliability improvement studies, c) supplier/subcontractor evaluations, d) component/part evaluations.

2. The contractor shall include reliability in trade studies in support of other program groups, such as system engineering, subsystem engineering, component design engineering, and parts engineering. The reliability support of these program groups shall include:

    a. Conceptual and detail system design configuration trade studies for system engineering

    b. Subsystem design configuration trade studies, alternate design approaches, and use of cross strapping for subsystem engineering

    c. Supplier/subcontractor reliability evaluations and internal component redundancy for component engineering

    d. Part reliability evaluations for parts engineering

3. The reliability trade studies shall be quantitative (i.e., with estimated reliability predictions) or qualitative (i.e., with a FMECA) or both.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

5.2.6 Manufacturing Reliability

1. The contractor shall evaluate the production and manufacturing operation process to ensure the hardware is manufactured in a repeatable and verifiable manner and will not degrade the planned reliability, using proven processes.

2. The contractor shall identify any production-critical processes (using process FMEA). These processes shall be previously qualified, proven, and identified on the manufacturing flow diagrams as a critical process.

3. The contractor shall identify all production critical purchased units, i.e., tooling, outsourced fabricated components, modified heritage/GFE. These units shall be controlled by qualified processes and internal procedures.

5.2.7 Reliability Assurance

5.2.7.1 Worst Case Analysis (WCA)

1. The contractor shall perform worst case analyses whenever a subsystem, component, or part cannot be shown by test and/or analysis to have adequate thermal, mechanical, and radiation design margins. The contractor shall utilize the worst-case parameter values and worst-case environmental operating conditions consistent with the mission.

2. The WCA on the electrical designs shall verify that the electronic circuits of components and subassemblies will operate successfully and have adequate design margins. These design margins shall take into account combinations of worst-case conditions, such as part tolerances (including drift), environmental (including radiation and temperature) and aging effects, and input/output extremes occur.

3. The contractor reliability organization shall coordinate with analysis performers to ensure that the analysis ground rules are followed and that the performer's planned methodology is acceptable and consistent with basic WCA procedures.

4. The independent review of the design by the Reliability Group shall include the mechanical and deployment designs, as well as the electrical designs.

5.2.7.2 Human Reliability Analysis (HRA)

1. The contractor shall identify the storage, handling, assembly, and test areas in the Launch site where a human performance deficiency could cause damage to the satellite and/or space/launch vehicle.

2. The contractor shall analyze the information from the FMECA, manufacturing process flow diagrams, and test and verification flow diagrams to identify critical human performance interfaces in the launch site operations. The contractor shall identify incidents that could degrade the reliability of the spaces/launch vehicle.

3. The contractor shall coordinate the findings of human factors, safety, reliability, and others in his organization that are in support of the launch site to provide preventive measures to mitigate the risk of these critical interfaces. This support shall include overseeing that the tasks are performed, as well as performing tasks directly related to reliability analyses.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

5.2.7.3 Fault Tree Analysis (FTA)

1. The contractor shall perform a FTA in those cases where the root cause of a failure is unresolved after normal engineering trouble-shooting and failure analysis efforts have been applied. The root cause failure analysis is part of the failure investigation and corrective action efforts. The areas of analysis shall include the manufacturing and testing processes, as well as the design and environment.

2. The FTA shall provide a detail analysis that systematically evaluates all possible failures and failure combinations in order to understand and show the possible root cause(s) of a failure.

3. A FTA shall be used to support the rationale for retention, as required, of critical items.

5.2.7.4 Part, Circuit, and Component Mechanical Stress Analysis

1. The contractor shall ensure that the reliability group interfaces with the design and PMP functions to ensure that the system, subsystems, components, circuits and parts have adequate design margins in stress derating, so that no item experiences maximum stress under worst case environmental conditions. The contractor will validate this by test and analysis. Any items that cannot meet these requirements shall be subject to worst case analysis.

2. The reliability group shall verify that all critical structural members and mechanical items have a positive margin of safety. Rationale and justification shall be made available for any critical structural member and/or mechanical item that does not have a positive margin of safety.

5.3 Testing and Reliability Evaluation

The contractor's reliability program shall be designed to coordinate with and evaluate the overall test program used to assess all aspects of the performance capability of the system and its elements under the anticipated mission environment and operating conditions. The contractor's reliability organization shall be responsible for the overall reliability evaluation program and for ensuring that accelerated and life test programs provide data and visibility in a timely manner for effective reliability evaluation at appropriate levels of assembly. The contractor's reliability effort shall also utilize the test results to support reliability analysis of the system.

The contractor's reliability program evaluation shall be coordinated with design, PMP, quality assurance, and manufacturing. The objective of this coordination shall be the exchange of qualification, acceptance, and failure data, to ensure a comprehensive test program from part selection to final system test, and to minimize or eliminate redundant or recurring testing. The reliability program shall:

a. Verify capability of the design to satisfy performance and environmental requirements without degrading reliability

b. Evaluate the susceptibility of the design and the hardware to failures, which could degrade reliability

c. Identify failure modes, which reflect deficiencies in materials, workmanship, or quality control

d. Review failure rates and other reliability data for impact on reliability

e. Validate the reliability of the hardware and software to function together to meet mission requirements

5.3.1 New Technology Qualification and Acceptance Testing

1. The contractor's reliability group shall review the process for conducting new technology qualification and acceptance testing of hardware containing new technology PMP to ensure that reliability deficiencies can be identified and corrected.

2. All test failures shall be investigated for root cause and coordinated with PMP and design engineering to evaluate the impact, if any, on reliability.

5.3.2 Environmental Stress Screening (ESS)

1. The contractor's reliability organization shall verify and ensure that an ESS process is developed and implemented to satisfy the ESS program requirements by reviewing and supporting the ESS effort. Specific reliability tasks associated with the ESS program shall include:

   a. Monitoring the ESS program and verifying the screening procedures to assure that the program is consistent with the ESS plans, technically sound, cost effective, and adequate measures are taken to remove defective screened items

   b. A review and verification of the hardware items identified and selected to be screened during the production phase, the screening measures to be applied, the test levels and durations, the performance and stress parameters to be monitored, the pass/fail criteria, and quantitative goals for the screening program. This review shall utilize results of development tests, defect history for similar items, technology in use, fabrication techniques, and FMECA results

   c. A review of the criteria used in selecting the hardware to be subjected to ESS

   d. Continuous reviews of the ESS process to ensure updates are made to reflect changes in environment parameters and manufacturing processes

2. The contractor's reliability organization shall implement documented procedures that define the contractor's methodology for:

   a. Determining the environmental stress levels sufficient enough to screen out latent defects that would otherwise be observed in the field

   b. Ensuring that all latent defects are mitigated prior to integration into the next, higher level of assembly

3. The contractor's reliability organization shall monitor the ESS tests during the production phase to ensure that anomalies and failures are detected, and the defective screened items are removed. Reliability shall document and report ESS failures as defined below.

a. Failures shall be documented in the project FRACAS, including failures to test support equipment and software.

b. ESS failures shall be reported to management in accordance with FRACAS reporting procedures, including identification of the root cause, corrective action, and lot number, serial number, or date the corrective action will take effect.

4. The contractor's reliability organization shall also quantify the risk of latent defects, if any, that remains in the product at delivery and their impact on field reliability. The reliability organization shall conduct defect trend analyses where necessary.

5. The contractor's reliability group shall utilize the ESS process to confirm that inspections and quality engineering have been performed properly. This information shall provide a feedback to the Manufacturing and Quality Assurance organizations on the effectiveness of their manufacturing and inspection processes.

5.3.3 Developmental Testing

1. The contractor shall plan a developmental test program that fully involves reliability engineering and shall submit the plan to the customer for approval. The planning shall occur as early in the design process as feasible, and inputs to the test plan shall include information from reliability predictions, FMEAs, and other reliability analyses. The test program shall be revised, as necessary, to reflect information on newly identified failure modes, emerging failure trends, design changes, production constraints, and operational scenarios.

2. The contractor shall conduct design verification tests of developmental hardware under conditions that simulate the function and the operational environment, plus adequate margin. Throughout developmental testing, the contractor shall document test failures in the FRACAS, analyze failure modes, and implement corrective action. The failures shall be reported to management in accordance with FRACAS reporting procedures and in accordance with contract provisions requiring delivery of test reports, reliability performance data, and other data deliverables.

3. Root cause analyses shall be performed by the contractor on test failures to identify the underlying causes of the failures so that effective corrective actions can be implemented to prevent recurrence. The contractor shall assess the test results to determine the achieved reliability of the test article and the system, and to identify any additional design or operational changes needed to meet reliability requirements.

4. On all system elements subject to developmental testing, the contractor shall ensure that items delivered by subcontractors are subject to sufficient testing to verify compliance with reliability requirements.

5. In the performance of this task, the contractor shall also demonstrate compliance with the contractor's lessons learned and best practices for design and test, confirm compliance with the reliability program, and identify lessons learned for dissemination to other projects. Test results and root cause analyses shall be provided to engineering organizations responsible for safety, reliability, logistics support, and sparing analysis, etc., and shall be retained for use in trend analysis and other reliability tasks.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

5.3.4 Reliability Life Testing

1. For new limited life hardware, the contractor shall design a reliability life test program and prepare a test plan for review and approval by the customer. The test program shall be documented and integrated with developmental testing and accelerated life testing (ALT) to ensure that maximum benefits are obtained from the overall test program. The contractor shall identify to the customer the hardware items that are candidates for life testing. If accelerated life tests are planned, the contractor shall identify the test and analysis methods, statistical models, and acceleration factor.

2. ALTs are conducted on components, materials, and parts to determine their useful life in the required product application, i.e., their purpose is not to expose defects, but to identify and quantify the failures and failure mechanisms that cause products to wear out before their calculated end of useful life. Because of this, ALTs must last long enough to cause the samples under test to fail. The test time may typically vary from a few weeks to a few months. ALTs usually take too long to be conducted on-line, as part of any product development cycle. Therefore, they must be conducted off-line, well before the components, materials, or parts are needed for a given application, conducted generically and using generic samples representing product components, materials, and processes.

3. The contractor shall perform tests under conditions expected during the life of the vehicle to determine the useful life span of the article under test. Life testing shall be performed after Preliminary Design Review (PDR), but prior to Critical Design Review (CDR), when flight-like surrogate hardware is available. Each test shall be conducted under nominal or accelerated operating conditions until failures are induced at a rate and severity indicating that the end-of-life has been reached for the test article. Where accelerated test methods are not used, the contractor shall augment the test program with compatible data, where available, from developmental testing or from tests on similar assemblies operating in similar environments. The reliability life-test-data shall be compared to design assumptions to validate the reliability predictions, determine whether product reliability requirements have been achieved, and identify candidate corrective actions.

4. The contractor’s reliability program shall be directly involved in the selection of test articles, use of statistical test planning techniques, test methods and conditions, and analysis methodologies.

Data items produced as a result of this task will be made available upon customer request. Appendix A provides information on potential data items related to this task.

APPENDIX A. RECOMMENDED TYPES OF CONTRACTOR RELIABILITY DATA ITEMS

Table A-1. CONTRACTOR RELIABILITY DATA ITEMS

Item	Part Reference	Data Item
Reliability Program Plan (RPP)	1.3	The RPP data requirements shall include the following items: a) A reliability program plan. This plan shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: • Initial submittal with the proposal • Revision submitted with negotiated changes 30 days after contract award • Updates and maintenance, as required, throughout the life of the reliability effort b) Reliability Status Reports. Reliability status reports shall be provided on a periodic schedule, per the CDRL or as negotiated.
Subcontractor/ Supplier Management, Surveillance, and Control Plan	5.1.3	The plan shall be included in Subcontractor/Supplier Management Plan or the Reliability Program Plan
Reliability Inputs to Formal Reviews/ Audits	5.1.4	The detail reliability data requirements for formal design reviews/audits are specified in the program reviews and audits compliance document titled "Technical Reviews & Audits for Systems, Equipment and Computer Software."
FRACAS Plan	5.1.5	This plan shall be included in the Reliability Program Plan and shall clearly describe the process for: a) Categorizing the failure b) Reviewing correctness of categorization decisions c) Prescribing levels of technical management judgment and review in the closure procedures for each failure category
FRACAS Status Summary Reports	5.1.5	These reports shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the FRACAS Status Summary reports shall be submitted with Reliability Progress Reports and prior to each readiness review after CDR.
FRACAS Reports	5.1.5	The FRACAS Reports shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the

Table A-1. CONTRACTOR RELIABILITY DATA ITEMS

Item	Part Reference	Data Item
		CDRL, the following schedule shall apply: a) The report shall be given orally, 24 hours after the failure occurrence b) Initial written report, shall be given within 3 working days c) Failure analysis and proposed corrective action given orally, as generated d) Closure report including failure analysis reports, due upon completion of required actions
Failure Analysis Reports	5.1.5	These reports shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the Failure Analysis Reports on parts or materials shall be included with the failure closure report.
Failure Trend Analysis Report	5.1.5	The failure trend analysis report shall be provided in the FRACAS Status Summary reports.
Failure Review Board Minutes	5.1.6	Minutes of each FRB meeting shall be prepared and distributed as directed by the customer.
Proof of Compliance Documentation on Previously Flown or Off-The-Shelf Hardware	5.1.7	The Proof of Compliance documentation shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the documentation shall be submitted with the proposal and at the formal design reviews.
System Reliability Prediction Report	5.2.1	A system reliability prediction report (including the detail reliability block diagram, detail reliability model and all supporting prediction inputs) shall be provided. This report shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: a) A submittal in the PDR data package. The prediction at PDR can be based upon component failure rates from a part's count failure rate estimate or from a contractor generic part failure rate list b) A submittal in the CDR data package. The prediction at CDR shall be based upon temperature-electrical stress component failure rate estimates for electrical components

Table A-1. CONTRACTOR RELIABILITY DATA ITEMS

Item	Part Reference	Data Item
Reliability Allocations	4.1.1	The reliability allocations shall be provided in the System Reliability Prediction Report and Reliability Status Reports.
FMECA Report	5.2.2	A system-level FMECA report shall be provided. This report shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: a) A submittal in the PDR data package. This FMECA report shall include a preliminary analysis on the components b) A submittal in the CDR data package. This FMECA report shall include: • A final FMECA on the components • The Support Equipment FMECA • A final system level FMECA c) Subsequent to CDR, any major design changes shall include an update to the FMECA report
Reliability Analysis of PMP	5.2.4	Any reliability analysis performed in support of the selection and/or verification of a part, material, or process shall be included with the PMP evaluation report.
Reliability Evaluation of Previously Flown or Off-The-Shelf Hardware	5.1.7	Hardware data and the reliability evaluation results shall be included in the documentation on Proof of Compliance for previously flown or off-the-shelf hardware.
Reliability Trade Analyses	5.2.1(3)	The results and narrative of the trade studies shall be provided in the System Reliability Prediction Reports.

Table A-1. CONTRACTOR RELIABILITY DATA ITEMS

Item	Part Reference	Data Item
Worst-Case Analysis Report	5.2.8.1	This report shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: a) A detail WCA report shall be provided in the PDR and CDR data packages. The PDR data shall consist of the WCA ground rules and methodology that will be used. The CDR data shall include the detail WCA b) Reliability verification of the WCA shall be provided in the Reliability Status Reports
Human Reliability Analysis Results	5.2.8.2	Human Reliability Analysis items shall be provided in the Reliability Status Reports.
Fault Tree Analysis (FTA) Results	5.2.8.3	The FTA results shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: a) The FTA for a root cause failure analysis support shall be provided with the applicable FRACAS report b) The FTA for critical items shall be provided with the analyses on the critical items
New Technology Qualification and Acceptance Testing	5.3.1	1. The contractor shall issue a report on the new technology qualification and acceptance test program. This report shall summarize the acceptability of the new technology for the intended application, and quantify the effect of the qualified technology on the reliability of the entire system, with supporting documentation. 2. Data from the qualification and acceptance level tests shall be retained by the contractor for future program use. 3. Failure data shall be input into the FRACAS process.
Environmental Stress Screening Failure Data	5.3.2	Failure data shall be input into the FRACAS process.

Table A-1. CONTRACTOR RELIABILITY DATA ITEMS

Item	Part Reference	Data Item
Developmental Testing	5.3.3	The Developmental Testing data items shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: a) The contractor shall provide a test plan, procedures, and reports in accordance with the program test schedule b) Failure data shall be input into the FRACAS process
Reliability Life Testing		The Reliability Life Testing data items shall be submitted per the Contracts Data Requirements List (CDRL). If a delivery schedule is not specified in the CDRL, the following schedule shall apply: a) The contractor shall provide test plans, procedures, and reports in accordance with the program test schedule b) Failure data shall be input into the FRACAS process
Failure Review Board (FRB) Close-Out Considerations	5.1.6	Remedial actions accomplished: Necessary preventive design and/or software changes have been devised and accomplished, and the pertinent engineering change notices referenced on the closeout documentation Necessary design or software changes have been verified in test Effectivity of preventive actions established Preventive actions made to existing identical items of hardware Closeout documentation signed-off by the appropriate management authority, which indicates technical review approval by the reliability and/or quality organization that certifies completion of all closeout actions
FRB DID/CDRL Considerations	5.1.6	An FRB charter that delineates the FRB's scope, objectives, authority, responsibilities, membership criteria, and procedures : The contractor shall apply the FRB requirements to applicable supplier/subcontractors FRB sessions shall be scheduled at regular intervals, and the customer shall be invited to participate in board deliberations as a voting member The scope of the FRB shall include verified contractor or subcontractor failure reports unless those parties have convened an FRB

Table A-1. CONTRACTOR RELIABILITY DATA ITEMS

Item	Part Reference	Data Item
Failure Review Board (FRB) Output Considerations	5.1.6	An FRB member shall be designated to chair the board. The FRB shall verify each failure occurrence and validate the report against the base-line system requirements. If a reported failure cannot be verified or validated, and no corrective action is appropriate, the failure shall still be reviewed and approved for closure, and such incidents shall be classified and tracked for trend analysis. If a reported failure is verified and validated, alternative corrective action measures may be offered for board consideration toward a consensus decision The FRB shall be granted the authority to delegate report verification, investigation, and analysis duties to competent project personnel The FRB shall ensure that its corrective action recommendations are submitted for approval by the designated project authority, and that a corrective action plan is implemented in accordance with a schedule Detailed description of each approved corrective action. Designation of the personnel responsible for implementing each corrective action. Schedule for initiating and completing each corrective action. Status report(s) on each in-progress corrective action. Report summarizing the results of each completed corrective action, including an assessment of its adequacy. Record of the failure report closure that includes an assessment of the residual risk.