



CLDP-PLN-3115
Revision A

Commercial Low-Earth Orbit Development Program Reliability, Maintainability, Logistics, and Supportability Management Plan Development Guide

Revision A

AUGUST 2025

This document has been approved for public release via the Scientific, Technical and Research Information DiscoverY System (STRIVES) 20250005472 Process. It has been reviewed for Proprietary, CUI, and Export Control (ITAR/EAR) and has been determined to be non-sensitive.

REVISION AND HISTORY

REV.	DESCRIPTION	PUB. DATE
-	Initial Release (Reference Directive CLDP-D0048, EFF. 04-17-25)	
	Program Release	04-21-2025
A	Revision A (Reference Directive CLDP-D0060, EFF. 08-27-25)	
	Program Release	08-27-2025

PREFACE

COMMERCIAL LOW-EARTH ORBIT (LEO) DEVELOPMENT PROGRAM (CLDP) RELIABILITY, MAINTAINABILITY, LOGISTICS, AND SUPPORTABILITY MANAGEMENT PLAN DEVELOPMENT GUIDE

The CLDP Reliability, Maintainability, Logistics, and Supportability Management Plan Development Guide provides to the Commercial Provider development guidance for a Reliability, Maintainability, Logistics, and Supportability (RMLS) Management Plan to be applied to their commercially developed, owned, and operated Commercial Low-Earth Orbit (LEO) Destination. The contents of this document are intended to be consistent with the CLDP Commercial Providers tasks and products.

This document is under the control of the CLDP Control Board (PCB). The PCB is the authority for baselining and approving changes. The NASA Office of Primary Responsibility (OPR) for this document is the CLDP Safety and Mission Assurance (S&MA) Office.

See Directive CLDP-D0060 Approval

08.27.2025

Angela T. Hart
Program Manager
Commercial LEO Development Program

Date

**COMMERCIAL LOW-EARTH ORBIT DEVELOPMENT PROGRAM
RELIABILITY, MAINTAINABILITY, LOGISTICS, AND SUPPORTABILITY
MANAGEMENT PLAN DEVELOPMENT GUIDE
CONCURRENCE
APRIL 2025**

Prepared by:	<u>Hector L. Chavez</u> BOOK MANAGER	<u>US</u> ORG
	<u>Hector Chavez</u> SIGNATURE	<u>04-09-2025</u> DATE
	Digitally signed by Hector Chavez Date: 2025.04.09 12:37:47 -05'00'	
Prepared by:	<u>Felisha Drake-Hill</u> BOOK COORDINATOR/DQA	<u>OP</u> ORG
	<u>Felisha Drake-Hill</u> SIGNATURE	<u>4/9/2025</u> DATE
Concurred by:	<u>Jenny R. Andrews</u> MANAGER, CLDP SAFETY & MISSION ASSURANCE	<u>US</u> ORG
	<u>Jay R. Andrews</u> SIGNATURE	<u>4/16/2025</u> DATE

TABLE OF CONTENTS

PARAGRAPH	PAGE
1.0 INTRODUCTION.....	1-1
1.1 PURPOSE.....	1-1
1.2 SCOPE.....	1-1
1.3 PRECEDENCE	1-1
1.4 VERB APPLICATION.....	1-1
2.0 DOCUMENTS	2-1
2.1 APPLICABLE DOCUMENTS.....	2-1
2.2 REFERENCE DOCUMENTS.....	2-1
3.0 RMLS MANAGEMENT PLAN DEVELOPMENT GUIDANCE	3-1
3.1 RELIABILITY	3-1
3.1.1 RELIABILITY QUANTITATIVE ANALYSES	3-2
3.1.1.1 RELIABILITY MODEL	3-2
3.1.1.2 RELIABILITY ALLOCATION.....	3-2
3.1.1.3 RELIABILITY PREDICTION	3-2
3.1.2 RELIABILITY QUALITATIVE ANALYSES	3-3
3.1.2.1 CRITICAL ITEM DATA.....	3-4
3.1.2.2 SINGLE POINT FAILURE ANALYSIS	3-4
3.1.2.3 REDUNDANCY ANALYSIS	3-5
3.1.2.3.1 COMMON CAUSES.....	3-5
3.1.2.3.2 REDUNDANT FUNCTIONALITY ASSESSMENT	3-5
3.1.2.3.3 REDUNDANCY TIMING ASSESSMENT	3-5
3.1.2.4 FAULT DETECTION, ISOLATION, AND RECOVERY VALIDITY	3-6
3.1.3 RELIABILITY TESTING	3-6
3.2 MAINTAINABILITY.....	3-7
3.2.1 DESIGN FOR MAINTAINABILITY	3-7
3.2.1.1 MAINTENANCE PROCEDURES	3-8
3.2.1.2 COMMON HARDWARE AND TOOLING	3-8
3.2.1.3 ACCESSIBILITY	3-9
3.2.2 MAINTENANCE CONCEPT AND PLANNING	3-9
3.2.2.1 MAINTENANCE CONCEPT GROUNDRULES	3-10
3.2.2.2 TYPES OF MAINTENANCE	3-10
3.2.2.2.1 PREVENTIVE MAINTENANCE	3-10
3.2.2.2.2 CORRECTIVE MAINTENANCE	3-11
3.2.2.2.3 CONTINGENCY MAINTENANCE	3-11
3.2.2.3 LEVELS OF ON-ORBIT MAINTENANCE.....	3-11
3.2.2.3.1 ON-ORBIT ORGANIZATIONAL MAINTENANCE	3-11
3.2.2.3.2 ON-ORBIT INTERMEDIATE MAINTENANCE	3-12
3.2.2.4 LEVELS OF GROUND MAINTENANCE	3-13
3.2.2.4.1 ORGANIZATIONAL MAINTENANCE LEVEL.....	3-13

CLDP-PLN-3115
Revision A

3.2.2.4.2	DEPOT MAINTENANCE LEVEL	3-13
3.2.3	MAINTAINABILITY ANALYSES	3-14
3.2.4	MAINTENANCE TRENDING	3-14
3.2.5	LIMITED LIFE ITEMS	3-14
3.2.6	REPAIR AND REFURBISHMENT	3-15
3.2.7	TEST, TEARDOWN, AND EVALUATION	3-15
3.2.8	SERVICE LIFE EXTENSIONS	3-15
3.3	LOGISTICS	3-16
3.3.1	ORBITAL REPLACEMENT UNIT SELECTION PROCESS	3-16
3.3.2	LOGISTICS CONCEPT AND PLANNING	3-1
3.3.3	LOGISTICS ANALYSIS	3-1
3.3.4	SPARES PLANNING AND SUPPORT ANALYSIS	3-2
3.3.5	RESUPPLY AND RETURN ANALYSIS.....	3-3
3.3.6	RESUPPLY AND RETURN PLANNING	3-3
3.4	SUPPORTABILITY	3-3
3.4.1	AVAILABILITY ANALYSES	3-4
3.4.1.1	AVAILABILITY MODEL.....	3-4
3.4.1.2	AVAILABILITY ALLOCATION.....	3-4
3.4.1.3	AVAILABILITY PREDICTION	3-4
3.4.2	FUNCTIONAL AVAILABILITY	3-4
3.4.2.1	FUNCTIONAL AVAILABILITY DETERMINATION	3-5
3.4.3	OBSERVED HARDWARE AVAILABILITY	3-5
3.5	USE OF PROBABILISTIC RISK ANALYSIS	3-5

APPENDIX

APPENDIX A	ACRONYMS AND ABBREVIATIONS.....	A-1
APPENDIX B	GLOSSARY	B-1
APPENDIX C	OPEN WORK.....	C-1
APPENDIX D	METRICS AND MATHEMATICAL MODELS.....	D-1
APPENDIX E	MODELING APPROACHES.....	E-1
APPENDIX F	ORBITAL REPLACEMENT UNIT SELECTION PROCESS.....	F-1

TABLE

TABLE C-1	TO BE DETERMINED ITEMS	C-1
TABLE C-2	TO BE RESOLVED ISSUES	C-1
TABLE D-1	RELIABILITY METRICS AND MODELING	D-1
TABLE D-2	MAINTAINABILITY METRICS	D-4
TABLE D-3	AVAILABILITY METRICS	D-5
TABLE E.4-1	CRITICALITY DEFINITIONS	E-4
TABLE E.4-2	COMMON CAUSE DEFENSE MECHANISMS	E-5

FIGURE

FIGURE E.1-1	FAULT TREE DIAGRAM EXAMPLE	E-1
--------------	----------------------------------	-----

CLDP-PLN-3115
Revision A

FIGURE E.2-1	RELIABILITY BLOCK DIAGRAM EXAMPLE	E-2
FIGURE E.3-1	EVENT TREE DIAGRAM EXAMPLE	E-3
FIGURE E.4-1	FAILURE MODES AND EFFECTS ANALYSIS METHODOLOGY	E-4
FIGURE E.5-1	FISHBONE DIAGRAM TEMPLATE.....	E-5
FIGURE E.6-1	PHYSICS OF FAILURE PROCESS IN DESIGN.....	E-6
FIGURE F-1	ORBITAL REPLACEMENT UNIT SELECTION PROCESS.....	F-1

1.0 INTRODUCTION

The National Aeronautics and Space Administration (NASA) is encouraging the development and growth of Commercial Low-Earth Orbit (LEO) Destination capabilities by promoting commercial competition. NASA plans to transition from ISS to Commercial LEO Destination operations and continue LEO research and development activities on commercially developed, owned, and operated Destinations. In the interim, NASA plans to offer Government Furnished Flights (GFF) (i.e., crew and cargo flight transportation services) for the first set of NASA missions with the expectation that Commercial Providers undertake and transition to an end-to-end Commercial LEO Destination service for the next set of missions. This document provides the Commercial Provider development guidance to develop and use a Reliability, Maintainability, Logistics, and Supportability (RMLS) Management Plan for their commercially developed, owned, and operated Commercial LEO Destination.

1.1 PURPOSE

The purpose of this document is to provide the Commercial Provider development guidance to develop and use a RMLS Management Plan for their commercially developed, owned, and operated Commercial LEO Destination.

1.2 SCOPE

The scope of this document applies to Commercial Providers development and use of an RMLS Management Plan for their commercially developed, owned, and operated LEO Destination.

1.3 PRECEDENCE

In the event of a conflict between this document and the commercial services contract requirements and/or applicable federally mandated laws and regulations, the commercial services contract requirements and/or applicable federally mandated laws and regulations take precedence.

1.4 VERB APPLICATION

The verbs are to be applied as follows:

- a) “Should” – Used to indicate good practice or a goal which is desirable but not mandatory.
- b) “May” – Used to indicate permission.
- c) “Will” – Used to indicate a statement of fact or declaration of purpose.
- d) “Is” or “Are” – Used to indicate descriptive material.

2.0 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents listed in this paragraph are applicable to the extent specified herein. Inclusion of applicable documents herein does not in any way supersede the order of precedence identified in Paragraph 1.3 of this document.

Document Number	Title
CLDP-REQ-1130	Requirements and Standards for the Commercial Low-Earth Orbit Development Program
CLDP-REQ-3102	Commercial Low-Earth Orbit Development Program Hazard Analysis and Safety Process Requirements Document
CLDP-STD-1150	Commercial Low-Earth Orbit Development Program Operations Standards<TBD 2-1>

2.2 REFERENCE DOCUMENTS

The following documents contain supplemental information to guide the user in the application of this document.

MIL-STD-1629A	Procedures for Performing a Failure Modes, Effects and Criticality Analysis
MIL-STD-756B	Reliability Modeling and Prediction
MIL-HDBK-472	Maintainability Prediction
MIL-HDBK-470A	Designing and Developing Maintainable Products and Systems
MIL-STD-781C	Reliability Design Qualification and Production Acceptance Tests: Exponential Distribution
MIL-STD-785B	Reliability Program for Systems and Equipment Development and Production
MIL-HDBK-1388	Logistic Support Analysis
MIL-HDBK-502A	Product Support Analysis
NASA/SP-2011-3421	Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

CLDP-PLN-3115
Revision A

NASA Version 1.1

Fault Tree Handbook with Aerospace Applications

3.0 RMLS MANAGEMENT PLAN DEVELOPMENT GUIDANCE

This document provides a Commercial Provider development guidance for an RMLS Management Plan to be applied to their commercially developed, owned, and operated Destination. This document identifies RMLS content and approach options available for a Commercial Provider to design and evaluate their Destination to ensure their commercially developed, owned, and operated LEO Destination performs for its design life at an acceptable level of risk.

3.1 RELIABILITY

The minimum expectation for reliability qualitative and quantitative assessments is to ensure the following have been correctly identified, evaluated, addressed, and accepted:

- A. Critical Items
- B. Single Failure Points
- C. Common cause events and mitigation
- D. Redundancy resiliency and effectiveness
- E. Fault detection, isolation, and response capability
- F. Controls

Reliability qualitative and quantitative analysis is used to design and evaluate systems (See Appendix D and E) to ensure systems perform as required, when required, for the required interval, and in the required environment, operating conditions, and expected usages; and tolerates faults, failures, and anomalous events to an acceptable level of risk to NASA.

As required by CLDP-REQ-1130, Requirements and Standards for the CLDP, the Commercial Provider is required to manage these risks using failure tolerance [R.CLDS.006, R.CLDS.029, R.CLDS.031, R.CLDS.098, R.CLDS.104, R.CLDS.248, R.CLDS.664, R.CLDS.197], prevention of failure propagation [R.CLDS.369, R.CLDS.324], and separation of redundant systems [R.CLDS.246, R.CLDS.665, R.CLDS.666]. The subsequent sections describe processes used to ensure system reliability and should be applied along with other engineering standards, processes, and methods including, but not limited to, controlling the selection and use of standard and non-standard parts through a parts program [R.CLDS.236], using materials and processes standards [R.CLDS.196], applying an environmental stress screening program (system exposed to environments such as ionizing radiation, etc. to stimulate failure mechanisms of defects), and managing and controlling the manufacturing and testing processes to ensure design requirements are met.

3.1.1 RELIABILITY QUANTITATIVE ANALYSES

Reliability quantitative analyses informs management the likelihood of a system or component failing over a specific period of time. The results of a reliability quantitative analysis can be used to identify potential design failure points and inform design change decisions to improve the overall reliability of a system or component by proactively addressing potential failure points, depending on where the failure point resides and how it propagates in the system. The results can be used to:

- Pinpoint failure points that may require a re-evaluation of the factors used to determine the probability of failure such as component lifetime, operating conditions, and stress levels.
- Identify critical components that are most likely to cause system failure that allow for focused improvement efforts.
- Evaluate different design options and guide the selection of an option with the highest predicted reliability.
- Understand the expected failure patterns so that maintenance schedules can be optimized to minimize system downtime and maximize system uptime.

3.1.1.1 RELIABILITY MODEL

The reliability model is a representation of a system design populated with reliability data that is analyzed to understand the system reliability and determine if design or operational changes are required to improve the system reliability (e.g., Appendix E.2 Reliability Block Diagram). The model needs to correctly represent the system to ensure that the analysis and results of the analysis informs the design and the decision process if design changes are needed to improve the reliability of the system.

3.1.1.2 RELIABILITY ALLOCATION

Reliability allocation is based on a realistic reliability goal set at the systems level and used to define the reliability requirements to design down to the next lower levels including the part level.

3.1.1.3 RELIABILITY PREDICTION

For non-maintainable items, reliability predictions are set at the lowest equipment level. For maintainable items, reliability predictions are determined down to the maintainable level (e.g., Orbital Replacement Unit (ORU)). Reliability predictions are based on historical or experiential performance data (e.g., accumulated operating times, cycle times, and/or attributable data), test results (e.g., test failures) and/or estimated using part or equipment level performance data. Failure rates are distinguished between demand-based failures (e.g., valve cycling, pyrotechnics) and time-based failure rates. Reliability predictions are updated over the life of the program based on operating experience. These reliability predictions are used to assess the overall system reliability, design trades, and to predict maintenance and sparing planning and supplies.

3.1.2 RELIABILITY QUALITATIVE ANALYSES

Reliability qualitative analyses identifies potential design and operational vulnerabilities that can impact crew safety or the mission (See Appendix E.4 Failure Modes and Effects Analysis). The vulnerabilities are identified to determine if and where improvements can be made at the system through the part level depending on where the vulnerability resides and how it propagates in the system. At a minimum, the reliability qualitative analysis applies to critical hardware. Reliability qualitative analysis is based on systematic identification of how the subsystem, component or equipment can fail, the causes for such failures, and the effects of these failures at each mission phase and be used to reduce the risks due to loss of function or degradation in performance and potential subsequent exposure to catastrophic and critical hazards (see CLDP-REQ-3102, CLDP Hazard Analysis and Safety Process Requirements Document). This includes ensuring that faults or failures are detectable and isolated, and the planned, mitigative response is achievable to protect crew safety or mission objectives given time to detect (TTD) and time to effect (TTE). Reliability qualitative analyses includes, but not limited to the following:

- System/Subsystem
- Interfaces
- Vendor/Supplier Impacted
- Part Name
- Part Identifier
- Part Function
- Failure Modes
- Failure Causes
- Failure Mechanisms
- Failure Effects (local, next higher level, end effects)
- Mission Phases/Operational Modes
- Critical Design or Operational Characteristics
- Severity
- Occurrence
- Fault Detection Method
- TTD
- TTE
- Criticality (see Appendix E, Table E.4-1, Criticality Definitions)
- Safety analysis cross-reference (see CLDP-REQ-3102)

CLDP-PLN-3115
Revision A

- Reliability quantitative analysis cross-reference
- Critical Item Determination

3.1.2.1 CRITICAL ITEM DATA

Reliability analysis is used to identify critical items. A critical item is one which, if defective or failed, directly contributes to a failure to meet crew safety, technical, programmatic, regulatory, or other stakeholder objectives. Critical items are tracked and managed using a critical items list (CIL). A CIL identifies, but not limited to the following:

- Tracking identifier
- Title
- Description
- Part name/drawing title
- Part number
- Quantity
- Related system and subsystem
- Criticality (e.g., represents consequence outcomes)
- Controls
- Supporting analysis, test results, documentation, and incidents
- Safety analysis cross-references (see CLDP-REQ-3102)
- Point of Contact (POC)/owner

3.1.2.2 SINGLE POINT FAILURE ANALYSIS

Single point failure (SPF) analysis identifies an independent element (e.g., single item or component) of the system whose failure results in a catastrophic or critical event (see CLDP-REQ-3102). SPF identification reveals what items are not redundant or have alternative mitigations in place to prevent catastrophic or critical events. SPFs are tracked, addressed, and residual risk documented to ensure that the residual risk has been reviewed and approved. SPF analysis includes, but not limited to the following:

- A. Identification of non-redundant critical items, common cause failure mode threats, and human error vulnerabilities.
- B. Documentation of the rationale and basis of SPF acceptance (e.g., reason for not designing out known SPFs)
- C. Tracking of SPFs (e.g., identifier, title, description, system/subsystem, criticality, part number, quantity, part name, drawing title, supporting analysis, test results, documentation, and incidents)
- D. Creations of a SPF list.

3.1.2.3 REDUNDANCY ANALYSIS

Redundancy analysis is an evaluation of multiple paths of performing the same function and determining the capability when one path fails where the item continues to function without loss of performance. Redundancy analysis identifies, describes, and records common causes, verifies redundancy functionality, affected redundant systems, separation of redundancy implementation, and redundancy verifications (e.g., redundancy testing). Redundancy analysis is done in tandem with an evaluation of detection capability and redundancy timing based on time to detect and time to effect constraints.

3.1.2.3.1 COMMON CAUSES

Common causes that can fail two or more redundant systems are identified and addressed. This includes developing and managing the implementation of verification plans to confirm that the common causes have been addressed. Common cause resolutions may include a separation of redundant paths implementation for items (i.e., liquid and gaseous systems, electrical systems, mechanical systems, and communication, command, and control systems) that prevents overlapping of paths vulnerable to a common cause event.

3.1.2.3.2 REDUNDANT FUNCTIONALITY ASSESSMENT

A redundant functionality assessment is used to determine if the redundancy approach effectively mitigates the worst-case failure effects prior to the failure effects manifesting. Operational and standby redundancy approaches are evaluated for effectiveness. Operational redundancy uses load sharing redundant items connected in such a manner that, upon failure of one redundant item, the remaining redundant items continues to perform the subsystem function and switching out the failed item is not required. Standby redundancy uses nonoperative (unpowered) redundant item(s) that become operational when they are (automatically or manually) switched into the subsystem upon failure of the primary redundant item.

Redundancy functionality assessment includes reviewing the redundancy verification plans used to verify the functionality of the redundancy, architecture description and system integration of the redundant systems, redundancy success criteria, and methods and tracking of any unresolved redundancy concerns that have been identified.

3.1.2.3.3 REDUNDANCY TIMING ASSESSMENT

Redundancy timing assessment includes an assessment of TTE and TTD to ensure redundancy is an effective means to prevent loss of critical functions. TTE is the time from failure occurrence to manifestation of the worst-case failure effect. TTD is defined as the estimated time from failure occurrence to detection of the failure. This redundancy timing assessment helps to understand and prepare crew for how much time they have to act between when a failure occurs and to understand what the effects of that failure might be. This assessment includes the timing analysis and tests to assure TTE and TTD is understood, acceptable, and implemented as designed.

3.1.2.4 FAULT DETECTION, ISOLATION, AND RECOVERY VALIDITY

The validity of fault detection, isolation, and recovery (FDIR) is evaluated to ensure that the redundancy strategy is implemented, and crew are informed and maintain a state of awareness of any failures that may occur. Fault detection is for item(s) whose loss can be detected at the functional recovery level by the flight or ground crew during any mission phase. Fault detection is applicable to the item under analysis and documents if the failure modes are detectable to allow timely switchover to the redundant item. The occurrence of a failure mode may be detected directly (e.g., position indicator detects that valve does not close), or indirectly from the resulting local or subsystem failure effects and then isolated to limit the effects of that failure. This evaluation ensures that the capability to detect and isolate failures that might affect their crew is effective. The evaluation would include fault isolation methods, fault detection methods, alert methods, accuracy of fault detection, system monitoring methods, threshold of nominal performance that triggers detection of failure, use of similar or dissimilar redundant hardware, coupling vulnerabilities between similar and dissimilar hardware (see common causes), recommended use of independent diagnostic tools, corrective action processes, problem definition approach, root cause analysis process, corrective action tracking, and concern tracking and closure process.

3.1.3 RELIABILITY TESTING

The development of a reliability testing strategy is dependent on what is required of the system being tested including such factors as criticality, impacts to safety and reliability, required level of reliability, maturity of the design, new technologies or processes, complexity, environments, and the ability to perform the testing under the required conditions. The basis for performing reliability testing addresses, but not limited to, the following:

- A. Understanding how the failure mechanisms occur and identifying a corrective action to prevent or reduce its occurrence.
- B. Determining if items or systems meet specified reliability requirements.
- C. Comparing estimated failure rates with failure rates derived from testing results.
- D. Monitoring reliability trends over time.
- E. Determining safety margin in a design.
- F. Estimating Mean Time Between Failures (MTBF) or Mean Time to Failure (MTTF) values.
- G. Identifying vulnerabilities in the design or parts.
- H. Ensuring that the item or system operates for its expected life.

A key component in enabling a reliability testing strategy is the development and use of a reliability test plan to define test objectives, range of testing, facilities, test requirements (test duration, number of units, number of allowable failures, acceptance

criteria), test schedule, test conditions, test monitoring, test participation, failure definition, test ground rules, and what and how test documentation is expected to be generated. Post-test analysis and results are then used to inform management and make decisions on any proposed changes to the design to improve reliability of the item or system.

3.2 MAINTAINABILITY

The minimum expectation for a maintainability qualitative and quantitative assessment is to ensure the following have been correctly identified, evaluated, addressed, and accepted:

- A. Critical system uptime and downtime
- B. Design for maintainability (accessibility, ease of de-installation, installation, etc.)
- C. Maintenance concept and planning
- D. Critical system maintenance preparation (hardware, tools, procedures)
- E. Identification of Limited Life Items (LLIs)
- F. LLI tracking, removal, and replacement.
- G. Repair and Refurbishment
- H. Service Life Extension

Maintainability qualitative and quantitative analysis is used to design and evaluate a system (See Appendix D) undergoing maintenance to ensure the system is retained in or restored to a specified condition within a given period of time (interval), where the maintenance is performed in accordance with prescribed procedures and resources. Given the interrelationship between maintenance and operations, CLDP-STD-1150, Operations Standards, is applicable when addressing maintainability to ensure maintenance operations applies a consistent and compatible approach when conducting maintenance and other supporting operations. The subsequent sections describe processes used to ensure system maintainability.

3.2.1 DESIGN FOR MAINTAINABILITY

Design for maintainability assures maintenance design and operations are considered early in the design and includes considerations for performance trending and analysis, fault or failure detectability and isolation, testability design, test point design, removal and replacement design, maintenance information management systems, physical accessibility, modularity, calibration, alignment, adjustment, standardization, interchangeability, human factors, use of common tools, limited support equipment, maintenance procedures, and personnel to facilitate maintenance during operations. Design for maintainability ensures fault detection, isolation, and recovery methods are identified and are part of the design; maintenance procedures include maintenance process and post-maintenance verification; tools, equipment, spares, etc., are identified that are required to do the maintenance; and maintenance is tracked to preclude

untimely failure of systems during their lifecycle. Inspection practices are critical in determining if or when maintenance is needed. Regular servicing and calibration of hardware prevents loss of functionality of the hardware throughout its life. Design for maintainability includes but not limited to the following:

- A. Preventive Maintenance (PM). PM should be minimized and require as little crew time as feasible. PM schedules should be flexible to accommodate changes in the schedule of other mission activities.
- B. Critical Hardware Redundancy. If maintenance is necessary and system operations are interrupted, redundant installations for critical hardware should be considered in order to permit maintenance without interrupting system operation.
- C. Minimize crew training.
- D. Minimize crew skill requirements.
- E. Minimize crew time spent on preventive and corrective maintenance.
- F. Increase maintenance capabilities during mission (especially corrective maintenance).
- G. Corrective Maintenance (CM). The benefit gained from repair should be worth the time and effort expended on repair. The time and effort involved in CM should be weighed against the cost and feasibility of carrying replacement units. Required calibration, alignment, or adjustment should be easily and accurately accomplished. Automate fault detection and isolation tasks whenever possible.

3.2.1.1 MAINTENANCE PROCEDURES

Maintenance procedures are developed and maintained to ensure actions are performed on equipment that requires removal and replacement or repair based on an item's specification. This may include periodic checks to verify that the equipment is operating within specification; identification of when the equipment requires maintenance to continue satisfactory performance; or replacement or repair to preclude a loss of function. The credibility of the maintenance action is assessed to ensure that potentially hazardous steps are identified and that the procedure places and maintains the system in a safe configuration.

3.2.1.2 COMMON HARDWARE AND TOOLING

Development and use of common hardware and tooling is considered in the design process to ease maintenance, minimize maintenance interval and system downtime (task efficiency), minimize tooling variety and quantity (e.g., minimizes cost), minimize logistics needs (e.g., no additional tooling needed), and optimize use of storage and staging locations (e.g., stowage capacity). Tool and test equipment commonality provides redundancy when multiple copies are available and contributes to crew readiness for unplanned maintenance activities. Interchangeable tools and test equipment improve mass efficiency because common items can cover multiple types of failures. Utilizing common tools and test equipment across vendors ensures tools and

test equipment are available where resupply constrains the ability to replace missing or ineffective tools and test equipment or where the ability to return maintenance items to the ground for maintenance is limited. Commonality ensures the tools and test equipment are available for a variety of maintenance events and improves crew familiarity with use and limitation of tools and test equipment and supports the development of common training to use these tools and test equipment, where applicable.

3.2.1.3 ACCESSIBILITY

Accessibility is the ease of which an item can be accessed during maintenance and may adversely impact maintenance times if not inherent in the design, especially on systems where on-orbit maintenance is required. When accessibility is not considered in the design, failures may occur caused by removal/disconnection and incorrect re-installation that hampers access to other items, causing rework. Accessibility is crucial for removal, replacement, and in-situ repairs (where an installed item is not designed to be removed). When designing for maintainability, accessibility considers visibility or may drive design characteristics that would aid blind removals or reinstallments. Accessibility can affect the ability to conduct tests post-installment of a replaceable item. Accessibility considers human factors design requirements to ensure access is compatible with crew needs to accomplish the maintenance tasks. The human factors identify structure and equipment features that impede maintenance task performance by inhibiting or prohibiting human body movement, and also identifies requirements necessary to provide an efficient workspace for humans who need the access to enable removal, replacement or repair. The system design needs to be specified and represented in drawings or sketches before detailed anthropometric evaluation can be effective. Early evaluation during concept development can assure early application of anthropometric considerations. Use of these types of evaluations results in improving access in designs largely in the areas of system provisions for equipment access, arrangement, assembly, storage, and maintenance task procedures. This effectively helps reduce time to effect repairs, lower maintenance costs, improve supportability systems, and improve safety.

3.2.2 MAINTENANCE CONCEPT AND PLANNING

The maintenance concept and planning enable management to consider design and operations early in the design lifecycle to ensure relative ease and economy of time and resources with which an item can be retained in or restored to a specific condition when maintenance is performed by personnel having specified skill levels, using prescribed procedures and resources, at each prescribed level of maintenance and repair. Items requiring maintenance are identified and how often that maintenance needs to occur for each item is determined. Ground and on-orbit maintenance is performed to sustain an acceptable level of system operability and to ensure system survival, crew safety, mission success, and utilization operations support. Corrective maintenance is also identified to restore system functionality following anomalies or equipment problems encountered during system operations or as a result of conditions discovered during

preventive maintenance. The primary mode of configuration maintenance on-orbit is the removal and replacement of failed items.

3.2.2.1 MAINTENANCE CONCEPT GROUNDRULES

- A. Maintenance is performed at the lowest level of the maintenance concept commensurate with the authorized personnel skills, tools and test equipment, repair parts, and technical documentation.
- B. Maintenance is accomplished within the following maintenance concept: on-orbit organizational, ground organizational, on-orbit intermediate, and depot.
- C. All levels of maintenance are accomplished in a manner that provides support of operational time constraints, prevents deterioration of acceptable operational levels of reliability and safety, ensures timely recycle of failed items to serviceable stocks, and accomplishes this support at minimum practical risk and cost. Maintenance records are updated with actual task times and activities.
- D. On-orbit maintenance forecasting includes the availability of on-orbit spares as identified by resupply and return analysis and availability of crew time as identified in on-orbit maintenance analysis.
- E. Ground depot level maintenance is accomplished by repair capabilities as determined by the Repair Level Analysis (RLA).

3.2.2.2 TYPES OF MAINTENANCE

3.2.2.2.1 PREVENTIVE MAINTENANCE

Preventive Maintenance (PM) consists of periodic routine maintenance actions performed on equipment which is operating within specification. It includes periodic checks to verify that the equipment is operating within specification or if the equipment requires periodic maintenance to continue satisfactory performance in order to preclude a functional failure. PM tasks include inspection, servicing, lubrication, calibration, and component time cycle or event cycle replacement prior to failure.

Specified PM tasks are considered requirements on the flight hardware, and performance of PM for its flight hardware within the required interval is mandatory. Deferral of PM is coordinated with safety and systems personnel and approved by management to ensure that the basis for the deferral is justifiable and the risks posed due to such deferral has been evaluated for acceptance.

PM on the ground also consists of periodic maintenance actions performed on equipment which is operating within specification. Ground PM is driven by flight requirements for ground checks. Ground PM tasks also include inspection, servicing, lubrication, calibration, and component time cycle or event cycle replacement prior to failure.

As in flight, designated ground PM is considered a flight hardware requirement for those items identified as requiring on ground prevention maintenance, and performance of this maintenance within its required interval is mandatory.

3.2.2.2.2 CORRECTIVE MAINTENANCE

Corrective Maintenance (CM) is performed to restore system functionality following anomalies or equipment problems encountered during system operations or as a result of conditions discovered during PM. The primary mode of CM on-orbit is the removal and replacement of the failed item. This primary mode can be supplemented by a repair of failed systems or subsystem hardware, or a repair of failed hardware which can be removed from its installed location.

CM on the ground is performed by the certified repair agency to restore the ORU to original performance standards. Upon receipt of the ORU at the designated repair facility, a test, teardown, and evaluation are performed as necessary to identify failed components requiring repair/replacement, and the results are reported out through the cognizant depot maintenance and repair interface. The report identifies repair recommendations that require the concurrence of the responsible representatives (engineering, S&MA, etc.).

3.2.2.2.3 CONTINGENCY MAINTENANCE

Contingency maintenance consists of temporary repairs performed in real-time with the resources available. Maintenance is contingent when restoration of critical functions is required to be performed without planned resources. Contingency maintenance would include manual bypass of automated mechanisms, repair using nonstandard parts or tools, and contingency ORU release. Contingency maintenance data includes available source data (e.g., maintenance planning and relevant engineering data). Contingency maintenance, to include controlled substitution, is performed on an exception basis through an approval process that includes coordination with safety, operations (e.g., flight director) and systems personnel and approved by management to ensure that the rationale for the exception is justifiable and the risk of performing a contingency maintenance activity is acceptable to crew safety and mission.

3.2.2.3 LEVELS OF ON-ORBIT MAINTENANCE

3.2.2.3.1 ON-ORBIT ORGANIZATIONAL MAINTENANCE

Organizational maintenance consists of functions and tasks that are performed on-orbit by crewmembers on installed systems or element flight hardware located either internally or externally. Organizational maintenance includes PM (e.g., crew checks, services, and scheduled maintenance services) and CM (replacement or in situ repair of failed components). Organizational maintenance also includes diagnosis and isolation of equipment malfunctions which can be readily traced to defective major assemblies/modular components using Built-in Test Equipment (BITE), go/no-go indicators, installed instrumentation, caution and warning indicators, or standard

diagnostic or fault isolation devices, such as volt Ohm meters. Organizational tasks include:

- A. Replacement of major assemblies or modular components on 1) a time change or condition monitored basis; and 2) those identified as worn, damaged, or otherwise defective.
- B. Anticipated alternate routing of interconnecting devices (e.g., cables and fluid lines, rather than replacement when alternative routing is significantly more efficient than replacement).
- C. Replacement of accessible, unserviceable piece parts not requiring special tools or test equipment (e.g., knobs, lamps, filters, and gauges).
- D. Performance of light structural repairs to include straightening, fluid line repair, and connector repair.
- E. Preparation for return to the ground for repair or replacement of the failed end items, major assemblies, and/or modular components which are beyond organizational repair capability or capacity.

3.2.2.3.2 ON-ORBIT INTERMEDIATE MAINTENANCE

Intermediate maintenance consists of functions and tasks that are performed on-orbit by Intravehicular activity crewmembers on system or element flight hardware which has been removed from their installed location. Intermediate level maintenance is planned in cases where significant improvement can be realized in maintenance upmass or system availability; and failures can be isolated below the ORU level using Built-in Test (BIT)/BITE, common portable test equipment, or analysis of the failure signature. In determining which ORUs to repair at the intermediate level, the benefits are compared to the additional crew time required, complexity of the repair, and potential hazard to crew or equipment. Intermediate level tasks include:

- A. Diagnosis and isolation of malfunctions; adjustment and alignment of modules which can be readily accomplished with test, measurement, and diagnostic equipment available on-orbit.
- B. Repair of equipment by replacing defective modular components and piece parts such as transistors, resistors, relays, coils, transformers, seals etc., when the replacement provides a high degree of reliability and successful return of the equipment to a serviceable status without extensive post-maintenance testing or adjustment.
- C. Repair of cables to include wire/optical splicing, pin straightening, replacement of worn insulation, etc.
- D. Repair of modular components limited to tasks requiring the servicing and replacement of seals, circuit boards, fittings, other external replacement parts and common hardware, and/or the application of authorized repair kits.

3.2.2.4 LEVELS OF GROUND MAINTENANCE

3.2.2.4.1 ORGANIZATIONAL MAINTENANCE LEVEL

Ground organizational maintenance consists of functions and tasks that are performed on ground equipment/support hardware that support launch processing, integration/de-integration of flight hardware, or ground testing of flight hardware. Ground organizational maintenance is typically restricted to one or more of the following activities:

- A. Fault isolation or detection to isolate or detect a fault or failure to a component level that can be efficiently replaced or repaired.
- B. Removal and replacement of major assemblies or modular components ORUs.
- C. PM services including visual inspections, lubrication, servicing, preserving, tightening, and minor adjustments to mechanical, electrical, fluid, and gas systems. This also includes the periodic replenishment of consumables or replacement of life-limited items.
- D. Replacement of piece parts.
- E. Verification activities necessary to ensure proper functional performance of equipment after a maintenance action has been completed.
- F. Flight hardware dispositioning after de-integration from the launch vehicle, including preparation for return to ground repair facilities.

3.2.2.4.2 DEPOT MAINTENANCE LEVEL

- A. This level of maintenance refers to tasks that are performed on the ground by a certified Depot for either GSE or flight hardware that has been removed or returned for service or repair.
- B. Depot maintenance includes:
 - 1. Diagnosis and isolation of malfunctions to the piece part level; adjustment, calibration, alignment, and repairs, as necessary.
 - 2. Replacement or repair of defective components which is beyond the authorized capability of other maintenance categories.
 - 3. Repairing modular components by replacing internal and external piece parts. This includes the replacement of printed circuit boards/cards constructed of conventional piece parts and selected solid state integrated circuits.
 - 4. Performance of heavy structural work.
 - 5. Overhaul/rebuild of end items/modular components.
 - 6. Repairs where manufacturing tolerances are required to be met and maintained or when special environmental facilities are required (e.g., clean room, hazardous material, controlled temperature/humidity special clothing, etc.).

7. Non-destructive testing to determine the utility of removed used parts. Special inspections, modifications of equipment, and periodic replacement of required life-limited components requiring extensive disassembly or elaborate test equipment. These are performed, when practical, as part of the cyclic overhaul or PM programs.

3.2.3 MAINTAINABILITY ANALYSES

Maintainability analyses informs management about the limitations on system or equipment downtime, maintenance labor-hours, and/or equipment availability. Downtime includes maintenance time (checkout, alignment, disassembly, reassembly, etc.), delay time (supply, administrative), and modification time. Duration-based parameters are evaluated such as mean time to repair (MTTR), which reflects mean of the times to repair weighted by the probability of occurrence mean time between maintenance activities and expected mean downtime (MDT), which is the mean active maintenance time (M), average supply delay time, and average administrative delay time (ADT). Maintainability analysis is used to optimize design and operations to reduce risks due to loss of function or degradation in performance and potential subsequent exposure to catastrophic and critical hazards.

3.2.4 MAINTENANCE TRENDING

Maintenance trends are tracked and reported. Using actual maintenance data, historical maintenance demands (maintenance actions and crew time) are compared against predicted demands. Predictions are shown both using original predicted reliability data and using updated data that considers the observed maintenance trends. The results of the data analysis are used to depict trends in hardware failures and support needs.

3.2.5 LIMITED LIFE ITEMS

Limited Life Items are components that need to be replaced during the life of the vehicle due to age or cycling. The Commercial Provider is responsible for tracking and updating the status of these items using a limited life items list (LLIL), tracking the remaining life on an item, and determining whether a PM removal and replacement is required prior to expected end of life or if a “run to failure” approach is acceptable. The Commercial Provider is also responsible for describing the process for identification of limited life items, planned method to address limited life items, and using a tracking method that identifies hardware design, testing, inspection controls, name and part number, usage area in the system, life-limiting characteristic(s) (how the life of the item is limited) and at what point in their life they need to be replaced, data sources, e.g., data sheets, LLI reports, acceptance data packages, and vendor/test data; expected life and supporting analysis or references; required life (provided by the design team, accounting for replacement refurbishment); refurbishment plans, restrictions, limitations (if applicable); and identifying limiting factors which determine the end of the life of the item including age degradation, cycle degradation, and consumables.

3.2.6 REPAIR AND REFURBISHMENT

Repair and refurbishment include issue identification, isolation to the maintainable unit, root cause and corrective action, and confirmation that the functional restoration has been achieved. Repair and refurbishment capabilities address a full cycle failure from its discovery to its correction as well as preventing failures. The repair and refurbishment process may use a standard method to perform root cause analysis, develop a resolution, and implement the correction action(s) required to address the issue. This includes assuring that the issue is tracked and closed when the corrective action(s) is taken and any subsequent methods to confirm the issue has been effectively addressed and that the corrective actions taken did not cause any other issues. Standard repair procedures are developed and maintained.

3.2.7 TEST, TEARDOWN, AND EVALUATION

Test, teardown, and evaluation (TT&E) is used to determine proximate cause (isolation of defects to the maintainable unit(s)) at a minimum and may be expanded to root cause identification. Assessments beyond proximate cause are used to determine whether the failure is indicative of limited life, the presence of a latent defect, and/or a candidate for an upgrade to the current design. Hardware is tested, then disassembled to be analyzed to determine its lifecycle parameters. TT&E can also be used identify if there are new failure modes or degradation levels throughout the lifecycle of the item. This information is used to determine if the failure rate estimations require updates. The TT&E process includes teardown planning and the use of test methods.

3.2.8 SERVICE LIFE EXTENSIONS

Service Life Extension is the ability to extend the life of the system beyond its original planned lifetime. Destinations expecting to operate beyond their original certified life, should identify critical original equipment manufacturing (OEM) data, test, and evaluations need to support life extension. Planning considerations include life-cycle maintainable systems, technology infusion, shelf life, identification of items not operationally capable beyond the life of the destination years with chance for extension, certification life extensions, and element replacement. Service life extension approach accounts for what risks would be involved in extending the service life of different items, how those risks are managed, and the analysis required to verify it is performed correctly (e.g., materials and structural analysis). This approach also addresses sustainability of items throughout the life of the system. Service life extension approach includes but not limited to the following:

- A. Description of the process to assess and extend service life, including criteria that would invalidate the continued operations (recertification) of any item beyond destination life with chance for exceptions.
- B. List of predeclared items that would be candidates for life extension and the conditions necessary for their extensions.

3.3 LOGISTICS

The purpose of logistics is to ensure systems are supported, maintained and operational. Logistics is required for planned maintenance, planned replacement of limited life items, and the replacement of failed items. The minimum expectation for a logistics qualitative and quantitative assessment is to ensure the following have been correctly identified, evaluated, addressed, and accepted:

- A. ORU Selections
- B. Minimum On-orbit and Ground Spares
- C. Maintenance Support Supplies
- D. Depot support (packaging, handling, ground transportation, staging, storage)
- E. Visiting Vehicle Transportation support (capacity, scheduling)
- F. Resupply and return analysis.

Logistics qualitative and quantitative analysis is used to design and evaluate the management, engineering, and technical activities and resources required to ensure system operations are sustained. The subsequent sections describe logistics processes used to sustain operations.

3.3.1 ORBITAL REPLACEMENT UNIT SELECTION PROCESS

When a maintenance concept includes the capability to restore on-orbit systems to an operational condition by the removal and replacement of ORUs, an ORU selection process needs to be developed and documented (see Appendix F).

3.3.2 LOGISTICS CONCEPT AND PLANNING

Logistics concept and planning includes logistics analysis, supply support planning and assessment, minimum on-orbit spares (MOOS) and ground spares planning and support analysis, and resupply and returning analysis and planning to define resupply return requirements. After the resupply return requirements are defined, items go through a prioritization assessment and manifest determination where competing items can conflict depending on the constraints and needs for the system that is required to be supported, maintained and remain operational. Once conflicts are resolved, the item is provisioned and delivered and placed into a tracking system. Ground support is required to ensure the readiness and availability of the support resources including inventory, packaging, handling, ground transport, staging, storing, procurement planning, repairs, tests, and personnel. Manifest planning accounts for flight transportation to and from the vehicle where the system resides that requires maintenance.

3.3.3 LOGISTICS ANALYSIS

Maintenance hardware delivery capability is planned and assessed to ensure supplies required to maintain on-orbit systems is available and items that are required to be returned to Earth are repaired, evaluated, and supported. ORU failure summary statistics is developed, managed, and controlled by function based on the logistics resupply cycle for both corrective and preventive maintenance which constrains the on-orbit maintenance planning. All systems and equipment requiring operational logistics support are logistics support analysis (LSA) candidates. The identification of candidate logistics carrier and support equipment items as line replaceable units (LRUs) is done by traditional maintenance analysis which starts with each item's Failure Modes and Effects Analysis and considers fault detection, isolation, and access and correction complexity in conjunction with packaging and economic alternatives. Logistic analysis is tailored by the level of maintenance. The logistics analysis considers the impacts on the limited on-orbit support resources such as crew man-hours, annual resupply return mass, on-orbit storage availability and criticality of the functions and systems which the logistics candidate supports. Logistics analysis identifies required logistics resources to support the systems and equipment. This analysis establishes the quantities of spares required on-orbit and on-ground to support operations and maintenance. An LSA candidate list is documented. LSA is provided for selected candidates. Basic LSA candidate items include, but are not limited to, the following:

- A. Equipment maintained as part of the system/equipment (on-equipment maintenance).
- B. Equipment maintained separately from the system, end-item, component, or subassembly with which they are functionally associated (off-equipment maintenance).
- C. Non-installed equipment to include support equipment.

- D. Groups of items may be maintenance significant while they would be disregarded on an individual part number basis.

3.3.4 SPARES PLANNING AND SUPPORT ANALYSIS

Spares planning and support is used to determine the required quantity of spares and ensuring support to deliver the spare to where it is needed (MOOS and ground spares). This includes spares planning, analysis, status, scheduling, quantity determination, and procurement as part of the overall sparing strategy. MOOS is an opportunity to understand what spares are needed to support continuous crew capability. Early in the lifecycle, MOOS may be used to initiate trades between inherent design/fault tolerance and spares and drive on-orbit stowage planning and decisions. Spares planning and support analysis includes, but not limited to the following:

- A. Spares quantity baseline estimation.

This is based on failure rates and component criticality. Quantity determination is determined by ORU predicted failure rate data. Based on the predicted failure rate, a time phased failure distribution model is developed. The final quantity determination is based on a combination of the results from the program ground-rules and assumptions, projected failures and Functional Availability (FA) inputs.

- B. Spares procurement or repair or refurbishment plan.

Determination of whether spares are procured and/or a spares repair or refurbishment capability is established. If design changes are required, procurement of upgraded parts/spares needs to be planned.

- C. MOOS or ground spares staging/storing plan.

Determination of whether spares are staged/stored on-orbit and/or ground and what type of staging/storing capability and capacity is going to be needed. This includes planning of packing configurations and options to stage/store packed configurations in available ground, flight transportation, and on-orbit locations.

- D. Spares production and scheduling plan.

Timing strategy of procurements (efficiency or just-in-time).

- E. Avoidance of obsolescence for vendor parts including technological obsolescence over time (i.e., loss processes, parts, or materials due to technological changes that may render replacements, repairs, or maintenance as unsustainable).

- F. Reliance on production diversion.

- G. Carrier availability, capacity, and scheduling.

- H. Configuration management.

To address changes that impact spares planning and support (technical changes, test and verification plan changes, assembly sequence changes, new failure rate information, and schedule changes).

3.3.5 RESUPPLY AND RETURN ANALYSIS

Resupply and return analysis is the systematic analysis of weight and volume requirements, which encompass delivery of ORU spares, repair parts, materials, support equipment, and tools to and from orbit, as well as associated on-orbit stowage requirements. The analysis is used to evaluate the capability to supply the necessary logistics support resources required to maintain on-orbit systems. These analyses are conducted using predictive models to simulate the maintenance demand over time, and the effect of applying logistics resources to meet that demand. Through adjustment of the assumptions and parameters of the simulations, various logistics support assessments can be performed. The sensitivity of weight and volume requirements can be assessed against factors such as flight rates, alternative logistics carriers, pre-positioned spares, and repair versus replace decisions. Re-supply and return analysis identify logistics resource drivers that are hardware items that demand significant re-supply, due to their failure rates and unit weight. Once identified, trade studies can be conducted to determine whether design changes are economically justifiable, and to assess their benefit. Trade studies are also conducted to identify alternate ways to deliver spares to orbit that relieves potential capability shortfalls. Resupply and return modeling is performed using engineering data, such as reliability and maintainability predictions, along with hardware weight and volume characteristics. In order to determine total system re-supply requirements, estimates are determined for hardware that has not yet had engineering data delivered. For these cases, if estimates are available, these are added to the modeling results. Estimates of resupply and return requirements also consider operational experiences. If no estimates are available, the system specification allocation values are used.

3.3.6 RESUPPLY AND RETURN PLANNING

Resupply and return planning is conducted at strategic, tactical, and incremental planning levels. At all levels, the planning process is iterative, the data matures and gains fidelity as the design matures and launch dates get closer. The results of the resupply and return analysis are used to provide projected up mass/down mass, volume, and on-orbit stowage requirements to planning documents. The up mass/down mass and volume requirements are integrated with other cargo categories, such as crew supplies, payload and facility hardware, consumables, etc. and compared to available capabilities. On-orbit stowage requirements include a projected list of on-orbit spares. The up mass/down mass, volume, and stowage requirements are updated as design development matures, and higher fidelity data is available. Resupply and return planning include items delivered to orbit (items that have failed or due for change out and limited life items).

3.4 SUPPORTABILITY

The minimum expectation for a supportability quantitative assessment is to ensure the following have been correctly identified, evaluated, addressed, and accepted:

- A. Critical functions

- B. Critical functions hardware availability reports if less than 100%
- C. Sparing quantities required to maintain availability to 90% or higher.

Supportability quantitative analysis is used to design and evaluate systems to determine if the system operates satisfactorily at a given point in time when used under stated conditions in the operational environment and not have any failure which cannot, through maintainability, be restored to operational service within a permissible time constraint. The subsequent sections describe processes used to ensure system supportability.

3.4.1 AVAILABILITY ANALYSES

The results of a systems availability analysis identify the percentage of time that a system is operating or is available to operate. Availability analyses informs management of candidate items or systems where a change can increase overall availability. The optimization opportunities are identified to determine if and where improvements can be made at the system through the part level depending on where the opportunity resides and its impact on the overall system availability. The availability analysis is based on systematic identification and prioritization of which subsystem, component or equipment availability can be increased to improve the overall availability.

3.4.1.1 AVAILABILITY MODEL

The availability model is a representation of a system design populated with availability data that is analyzed to understand the system availability and determine if design or operational changes are required to improve the system availability. The model needs to correctly represent the system to ensure that the analysis and results of the analysis informs the design and the decision process if design changes are needed to improve the availability of the system.

3.4.1.2 AVAILABILITY ALLOCATION

Availability allocation is based on a realistic availability goal set at the systems level and used to define the availability requirements for design down to the next lower levels including the part level.

3.4.1.3 AVAILABILITY PREDICTION

Availability predictions are accomplished at the lowest equipment level and are based on historical or experiential performance data, test results, and/or estimated using part or equipment level performance data. Availability predictions are used to assess the overall system availability and design trades.

3.4.2 FUNCTIONAL AVAILABILITY

Functional Availability (FA) is calculated using predictive data including reliability data, flights per year, repair time, etc. FA is used to aid in the determination of spare quantities, assess real-time system performance, and to assess requirements for

resources for maintenance such as crew time, upmass, carriers, etc. As a goal, sparing quantity can be determined based on system availability of 90% or higher.

3.4.2.1 FUNCTIONAL AVAILABILITY DETERMINATION

The demand for spares is evaluated on a periodic basis. The evaluation considers original predicted reliability data, updated reliability data (which takes into account actual performance to date), characteristic life (for wear out failure modes), preventive maintenance requirements, and estimates for environmentally induced failures. For FA assessments, the functional architecture and the impact of each ORU on the overall availability of the function is considered. The assessment evaluates quantities of spares required to maintain the defined target levels. By comparing existing program assets and plans (spares, repairs, etc.) against the assessment derived spares demands, the sparing risks can be identified and addressed. The spares assessment results are considered along with judgment of sub-system experts and program maintenance resources to identify options, recommend, prioritize and plan activities to increase spares quantities. Critical functions are predefined to ensure that the function architecture representation is correct and usable.

3.4.3 OBSERVED HARDWARE AVAILABILITY

Observed hardware availability is reported to evaluate how effectively the system is being supported and to ensure that it can perform its intended services. Hardware availability is a snapshot of the percent of ORUs in a function that are operable at the particular point in time that is being reported. The operational status of the system is reported by function.

3.5 USE OF PROBABILISTIC RISK ANALYSIS

Where reliability analysis focuses on a system's ability to perform its function reliably over a specified period, probabilistic risk analysis (PRA) assesses the likelihood and potential consequences of various risks. Both use similar methods (e.g., fault tree analysis, event trees) but apply such methods for a different purpose and scope. PRA is used to estimate risk to crew safety and mission success with limited information. PRA is a comprehensive, structured, and disciplined approach to identify and analyze risk in engineering systems using identified and defined events or scenarios which can occur. The PRA begins with an initiating event and uses interim pivotal events to arrive at multiple end states. These models are populated with estimated probability of an event or scenario occurrence (likelihood) limited by the degree of doubt or lack of knowledge about the outcome (uncertainty) then branches out to the next pivotal event based on the success or failure of the prior event to arrive at multiple end states (e.g., resulting outcomes may include significant safety consequence events). An event tree can be used to show how an initial event progresses through each of the pivotal events until an end state is achieved (See Appendix E.3, Event Tree Analysis). The purpose of a PRA is to assess probabilities, identify vulnerabilities, and ultimately, improve safety. PRA uses probabilistic methods including fault trees, event trees, and Monte Carlo simulations to analyze potential failure scenarios.

APPENDIX A - ACRONYMS AND ABBREVIATIONS

ADT	Administrative Delay Time
BIT	Built-In Test
BITE	Built-In Test Equipment
CCP	Commercial Crew Program
CFE	Contractor Furnished Equipment
CIL	Critical Item List
CLDP	Commercial LEO Development Program
CM	Corrective Maintenance
e.g.	For example,
EI	End Item
Etc.	Etcetera
EVA	Extravehicular Activity
EVR	Extravehicular Robotic
FA	Functional Availability
FDIR	Fault Detection, Isolation and Recovery
FI	Fault Isolation
FMEA	Failure Modes and Effects Analyses
FMECA	Failure Modes, Effects, and Criticality Analysis
FSE	Flight Support Equipment
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GSE	Ground Support Equipment
GPMC	Governing Program Management Council
ILS	Integrated Logistic Support
ISS	International Space Station
IVA	Intravehicular Activity

CLDP-PLN-3115
Revision A

K-Factor	K-Factor
LEO	Low-Earth Orbit
LLI	Limited Life Item
LLIS	Limited Life Item List
LRU	Line Replaceable Unit
LSA	Logistics Support Analysis
LSAR	Logistics Support Analysis Record
MBSE	Model Based Systems Engineering
MDT	Mean Downtime
MIL	Military
MMOD	Micro Meteoroid Orbital Debris
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
OEM	Original Equipment Manufacturer
ORU	Orbital Replacement Unit
OSE	Orbital Support Equipment
PM	Preventive Maintenance
POC	Point of Contact
R&M	Reliability & Maintainability

CLDP-PLN-3115
Revision A

RBD	Reliability Block Diagram
RBDA	Reliability Block Diagram Analysis
RCM	Reliability Centered Maintenance
RMLS	Reliability, Maintainability, Logistics, and Supportability
S&MA	Safety and Mission Assurance
SPF	Single Point Failure
SRU	Shop Replaceable Unit
TBD	To Be Determined
TBR	To Be Resolved
TD&D	Technical Data and Documentation
TTD	Time to Detect
TSE	Test Support Equipment
TTE	Time to Effect
TT&E	Test, Teardown, and Evaluation
U.S.	United States

APPENDIX B - GLOSSARY

ANOMALY

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

AVAILABILITY, OPERATIONAL

Operational availability (A_o) is 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 CM downtime. This value is equal to the MTBF divided by the MTBF plus the 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

Inherent availability (A_i) is 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 CM time. It excludes logistics time, waiting or administrative downtime, and preventive maintenance downtime. It includes CM downtime. Inherent availability is generally derived from analysis of an engineering design and is calculated as the MTTF divided by the MTTF plus the MTTR. It is based on quantities under control of the designer.

CONSUMABLES

See CLDP-REQ-1130, Appendix B, Glossary, Consumable.

CONTINGENCY

For planning, an emergency or urgent need that is regarded as unlikely but requiring some extent of pre-determined action if it occurred.

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).

CONTINGENCY MAINTENANCE

Maintenance that is required to be performed without planned resources available.

CORRECTIVE MAINTENANCE

Maintenance performed to restore system hardware integrity following anomalies or equipment problems encountered during system operations or as a result of conditions discovered during preventive maintenance.

CRITICAL

A condition where a failure occurrence can result in loss of life, serious personal injury, loss of mission, or loss of a significant mission resource or objectives.

CRITICAL HARDWARE

Any hazardous or safety critical equipment or system. See CLDP-REQ-1130, Appendix B, Glossary for the definition of safety-critical.

CRITICAL ITEM

A critical item is one which, if defective or fails, directly contributes to a failure to meet crew safety, technical, programmatic, regulatory, or other stakeholder objectives.

CRITICAL ITEM LABEL

Placed on Class I, II, and III interior packaging and exterior shipping containers to alert all shipping and handling personnel on the criticality of the item.

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.

DEFERRED MAINTENANCE

Authorized delay of maintenance/repair of uncorrected equipment failures.

DEPENDABILITY

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

DEPOT LEVEL MAINTENANCE

The designated maintenance level which has the capability to perform corrective and preventive maintenance of ORUs/Line Replaceable Units (LRUs)/SRUs and designated equipment utilizing support equipment, facilities, personnel and skills that are not economically available at other maintenance levels. Depot maintenance consists of repairs made to hardware that has been removed from its installed location and returned to the ground and includes repairing, overhauling, modification and calibration of equipment.

DESIGN DEVIATION

Any deviations between actual hardware configuration and baselined design.

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.

EVENT TREE ANALYSIS

Event Tree Analysis (ETA) is a forward, top-down, logical modeling technique that explores potential outcomes stemming from a single initiating event, helping to assess probabilities and understand system behavior.

EXPECTED LIFE

The estimated operational life of an item based on its use and the environmental and operating conditions, etc. for the given mission; or the rated life (i.e., data provided by the manufacturer/supplier/vendor based on heritage or life testing).

FAILURE

See CLDP-REQ-1130, Appendix B, Glossary, Failure.

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

Failure modes and effects analysis (FMEA) is [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. FMEA is [2] an analysis to identify potential design weaknesses through systematic, documented consideration of the following: all likely ways in which a component or equipment can fail; causes for each mode; and the effects of each failure (which may be different for each mission phase). FMEA is [3] an 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 MODES, EFFECTS AND CRITICALITY ANALYSIS

Failure modes, effects and criticality analysis (FMECA) is 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

See CLDP-REQ-1130, Appendix B, Glossary, Failure Tolerance.

FAULT

See CLDP-REQ-1130, Appendix B, Glossary, Fault.

FAULT DETECTION, ISOLATION, AND RECOVERY

Fault detection, isolation, and recovery is the identification of a hardware anomaly occurring in an operating system (mechanical, electrical, or electronic), the tracking down of the anomaly to a specific hardware item within a system, the repair process/procedure to return the hardware item/system to its fully operational condition.

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

Fault tree analysis (FTA) is 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 occurs, 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.

FAILURE VERIFICATION

Means by which the cause of the failure was determined.

FLIGHT SUPPORT EQUIPMENT

Flight support equipment (FSE) is equipment, both hardware and associated software/procedures, which has been designated to be used to provide on-orbit and in-flight support to the flight element/hardware and then are returned to the ground.

FUNCTIONAL AVAILABILITY

Functional availability (FA) is a performance measure for assessing resources for maintenance because it directly relates operational scenarios to quantifiable measures of performance.

GOVERNMENT FURNISHED EQUIPMENT

Government furnished equipment (GFE) is equipment in the possession of, or acquired by the government, and delivered or otherwise made available to a non-Governmental or Governmental organization.

GROUND SUPPORT EQUIPMENT

Ground support equipment (GSE) is equipment, both hardware and associated software/procedures, which is used on the ground to provide some means of support to flight systems or equipment. GSE includes test and checkout equipment, handling and transporting equipment, access equipment, and servicing equipment.

HARDWARE

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

INCREMENT

The duration of an increment is the time period starting immediately after the undocking of a transportation vehicle to, and including, the undocking of the next transportation vehicle. The calculation of increment duration begins by counting the day after undocking of a transportation vehicle as day one of the increment. The calculation of increment ends on and includes the day of undocking of the next transportation vehicle. An increment can support one (1) or more stages; usually an increment consists of (2) two stages where the number of crew may differ (e.g., 3 then 6 crewmembers).

INSITU MAINTENANCE

Maintenance performed at the location of the failed item/function.

INTEGRATED LOGISTICS SUPPORT

Integrated logistics support (ILS) is the process through which the composite of management and analysis actions necessary to assure effective and economical support of the system, both before and after assembly, are accomplished.

INTERMEDIATE MAINTENANCE

Intermediate maintenance consists of repairs to failed hardware that has been removed from its installed location. Intermediate maintenance is performed on-orbit, but only in the internal environment. It may be performed on external hardware that has been transferred inside for repairs.

INTERMEDIATE ON-ORBIT LEVEL OF MAINTENANCE

The designated on-orbit level of maintenance that is responsible for corrective and preventive maintenance of ORUs removed from their installed location. Item failures are normally repaired by disassembly, repair and reassembly of the item. Intermediate maintenance is considered the middle level of maintenance and supports the Organizational on-orbit level of maintenance.

INTRAVEHICULAR ACTIVITY MAINTENANCE

Intravehicular activity (IVA) maintenance takes place within the pressurized modules. IVA maintenance can be done on external equipment brought into the pressurized environment. Baseline IVA maintenance is removal and replacement, preventive maintenance actions, in situ repair, or repairs at the maintenance work area.

K-FACTOR

A multiplier that is used to de-rate the MTBF based on expected non-inherent failures (Micro Meteoroid Orbital Debris (MMOD), Human and hardware induced, false rate, etc.).

LEVEL OF REPAIR ANALYSIS

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

LEVELS OF MAINTENANCE

Designation of sites where maintenance is performed based on the capabilities and resources available. These levels have been designated as (1) Organizational on-orbit, (2) Organizational on-Ground, (3) Intermediate on-orbit, and (4) Depot.

LIFE LIMITING CHARACTERISTIC

The environmental, use, or other factor that limits the life of the item, e.g., time, operating time, actuations, or revolutions.

LIFE RATIO

The ratio between the Expected Life and the Required Life: $\text{Life Ratio} = \frac{\text{Expected Life}}{\text{Required Life}}$.

LIMITED CALENDAR LIFE ITEM

Any item that deteriorates with the passage of time, i.e., items susceptible to aging. This includes installed as well as stored items.

LIMITED LIFE/LIFE LIMITED

Designations referring to an item with limited useful life, regardless of whether the limitation is due to operational consideration, calendar life, or a combination.

LIMITED LIFE ANALYSIS

Analysis performed to assess the risk to mission success/objectives resulting from the use of limited life items.

LIMITED LIFE ITEM

Any item (component or material) designated as having a limited useful life regardless of whether it is a limited operating life, limited calendar life, operating parameter sensitive, or combination.

LIMITED LIFE ITEMS LIST

A list of all limited life items identified by the analysis and their corresponding characteristics (e.g., expected life, required life, and life ratio).

LIMITED OPERATING LIFE

Any item that deteriorates with increased accumulation of operating time/cycles and thus requires periodic replacement or refurbishment to assure that its operating characteristics have not degraded beyond acceptable limits. This includes consideration for total mission time/cycles and safety factor margins.

LINE REPLACEABLE UNIT

A line replaceable unit (LRU) is a unit of hardware that is designated to be removed and replaced to maintain a ground support system in its operational condition. Applies to non-flight hardware.

LOGISTICS

The management, engineering, and technical activities concerned with determining requirements, system design, and supplying and maintaining resources to support objectives, plans and operations.

LOGISTICS ENGINEERING

Those support related activities that deal primarily with system design and development. Such activities include the initial establishment of logistics support requirements (i.e., criteria and constraints), the development of the maintenance concept, the allocation of support requirements, LSA, the design for system supportability, the design and development of new elements of logistics support (e.g., test equipment, facilities, etc.), and the test and evaluation of the system support capability. In essence, logistics engineering covers (1) the design of the prime mission equipment for supportability, and (2) the design of the overall support capability for the system.

LOGISTICS SUPPORT ANALYSIS

Logistics support analysis (LSA) is an iterative, analytical process through which support considerations impact system and equipment design, and operational support resources and requirements are identified.

LOGISTICS SUPPORT ANALYSIS RECORD

Logistics support analysis record (LSAR) is that portion of LSA documentation consisting of detailed data pertaining to the identification of logistics support resource requirements of a system or element.

MAINTAINABILITY

A characteristic of design and installation which inherently provides for the item to be retained in or restored to a specified condition within a given period of time, when maintenance is performed by prescribed procedures and resources. 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 is 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. The function of keeping items or equipment in, or restoring to, a specified operational condition. It includes servicing, test, inspection, adjustment/alignment, access, assembly/disassembly, lubrication, operation, decontamination, removal, replacement, installation, fault location, calibration, condition determination, repair, modification, overhaul, rebuilding, and reclamation. Maintenance includes both preventive and CM for both on-orbit and on-ground.

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.

MAINTENANCE CONCEPT

Narrative description identifying the broad, planned approach to be employed in sustaining the system/equipment at a defined level of readiness or in a specified condition in support of the operational requirements.

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 retains 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.

MISSION LIFE RISK

The possibility of premature failure or margin loss due to use, environment, or aging.

MITIGATION

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

NEXT HIGHER ASSEMBLY

The larger assembly that a part is directly installed into where a part refers to a single, individual component and the assembly using this part is called the next higher assembly.

OBSOLESCENCE

The loss or impending loss of the last known manufacturer or supplier of raw material, production parts or repair parts.

ON-ORBIT INTERMEDIATE MAINTENANCE

Any on-orbit maintenance activity that requires the penetration of an ORU's envelope or that requires maintenance.

ON-ORBIT ORGANIZATIONAL MAINTENANCE

Maintenance that is performed by the flight crew on installed system or element flight hardware in either pressurized or unpressurized environments to sustain the on-orbit systems and element readiness.

OPERATING PARAMETER SENSITIVE ITEM

Any item that has a limited life due to variances in its operating parameters that may not be directly related to operating or calendar time.

OPERATIONAL READINESS

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

ORBITAL REPLACEABLE UNIT

An item which can be removed and replaced as a unit at the on-orbit organizational level of maintenance.

ORGANIZATIONAL GROUND LEVEL OF MAINTENANCE

The designated ground level of maintenance that is responsible for corrective and preventive maintenance of ground support equipment and systems during ground processing. Systems failures are normally corrected by removing and replacing failed items (ORU/LRUs) or in-situ repair.

ORGANIZATIONAL MAINTENANCE

Organizational Maintenance is performed on hardware in its installed location and may include removal and replacement of failed hardware or in situ repair. Organizational maintenance may be performed on-orbit or on the ground. On-Orbit organizational maintenance may be performed in either the internal environment (IVA) or the external environment. Maintenance in the external environment may be performed by a crewmember (EVA) or by/with the assistance of robotic systems (EVR).

ORGANIZATIONAL ON-ORBIT LEVEL OF REPAIR

The designated on-orbit level of maintenance that is responsible for orbital systems corrective and preventive maintenance. System failures are normally corrected by removing and replacing failed items (ORUs) or in-situ repair. Maintenance performed on-orbit by crewmembers on installed system or flight hardware in either pressurized or unpressurized environments. This level includes internal and external maintenance performed by external robotic capability, EVA human, external robotic/EVA human cooperative, and IVA human.

PACKAGING

Application or use of adequate protective measures to prevent damage from physical hazards or conditions including wrapping for protection from physical danger, bagging

CLDP-PLN-3115
Revision A

and/or desiccating to protect from environmental conditions, cushioning interior containers, and complete identification markings of unit and intermediate packages or containers.

PREPOSITIONED SPARES

Those hardware items used in a replacement maintenance task that are stowed in a location prior to a hardware failure.

PRESERVATION

Application or use of adequate protective measures to prevent deterioration from environmental hazards or conditions including, as applicable, the use of appropriate cleaning and drying methods, preservatives, and wrappings.

PREVENTION

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

PREVENTIVE MAINTENANCE

Scheduled routine maintenance actions performed on equipment which is operating within specification and requires periodic maintenance to continue satisfactory performance or preclude failure.

PROBLEM CAUSE

Reason for failure (e.g., electrical short due to damaged wiring insulation, mechanical failure, loss of coolant due to leak, etc.).

Problem/Failure/Anomalies 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.

PROCEDURE DEVIATIONS

Any differences between defined SODF procedures and actual procedures performed which were necessary to complete the required maintenance task.

PROCUREMENT

The obtaining and delivery of equipment, spares and materials.

PRODUCT

Hardware, software, services or data that are provided to the customer.

PRODUCT DIVERSION

Hardware assets delivered in advance which are diverted and used to fulfill replacement demands.

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.

PROVISIONING

A disciplined process that identifies types and quantities of spares, repair parts, and consumables items that should be procured and stocked to sustain and maintain equipment and systems for a specific period of time.

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 fails 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 performs 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

Reliability Block Diagram Analysis (RBDA) is 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

Reliability centered maintenance (RCM) is 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 CM and minimize preventive maintenance.

REPAIR

A series of CM tasks required to return an item or function to a serviceable condition.

REPAIR TIME

Time required to perform maintenance task.

REPLENISHMENT

The process of pricing, ordering, and stocking spare parts needed to maintain, overhaul, or repair a major system over its life based on the initial provisioning list and demand and usage patterns established on during the initial provisioning period. It may be accomplished by either the Government or a designated contractor.

REQUIRED LIFE

The life the item is required to meet including storage, testing, operation, duty cycle, maintenance, and refurbishment considerations for the given mission.

REQUIREMENTS

Requirements are statements of need that define what a system does and how well it performs those tasks.

RESUPPLY AND RETURN ANALYSIS

A systematic analysis of weight and volume, which encompasses delivery of ORU spares, repair parts, material, support equipment and tools to and from orbit and any associated on-orbit stowage requirements.

RESUPPLY/RETURN OPERATIONS

Operating functions that are associated with logistics resupply of the system and the return of items to Earth.

REVIEW

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

RISK

See CLDP-REQ-1130, Appendix B, Glossary, Risk.

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. See CLDP-REQ-1130, Appendix B, Glossary, Safety-Critical.

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.

SHOP REPLACEABLE UNIT

A unit of hardware that is designated to be removed and replaced to maintain an on-orbit system in its operational condition.

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.

SOURCE DATA

Any approved or released documentation which is used in the development of LSAR and technical data and documentation (TD&D). Source data consists of subcontractor released documentation, such as: engineering drawings, specifications, Data Requirements, other manuals, specially released engineering documentation supplied for information, close-out photographs and videos, and graphics.

SPARES

Replacement hardware items used to maintain system operations by repairing, replacing, or restoring (repairing) system functions (preventive and CM). Maintenance replacements for parts, components, or assemblies in deployed items of equipment.

SPECIALIZED CONTAINER

Specialized Containers are uniquely configured to support and protect a specific item during handling, storage, and shipment. Specialized containers frequently incorporate energy absorbing systems, temperature and humidity control systems, or special features to make handling or shipment possible, easier or safer.

STRATEGIC, TACTICAL AND EXECUTION PLANNING

mA phased process of determining cargo requirements beginning with broad long range annual allocations followed by a year's cumulative allocations by incremental and culminating in a specific mission manifest.

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. Equipment used to transport, handle, support, protect, maintain, or service hardware/software, on-orbit or on the ground. Deliverable support equipment is categorized as FIGHT flight support equipment (FSE), orbital support equipment (OSE) and GSE.

SUPPORTABILITY

Relates to the degree to which the system can be supported, both in terms of the inherent characteristics of prime equipment design and the effectiveness of the overall support capability (i.e., elements of logistics support). Supportability is assessed through availability analysis that overlaps with reliability, maintainability, and logistics.

SUSTAINABILITY

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

SUSTAINING ENGINEERING

Activities performed to keep the system within specifications or return it to design specification. Includes system performance analysis, systems analytical model maintenance, system performance assessment, and system modification development and integration.

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

See CLDP-REQ-1130, Appendix B, Glossary, Test.

TEST/RETEST

Means by which restoration of functionality was verified.

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.

TIMELINE

A graphical representation of the temporal relationships of activities or functions. Horizontal bars indicate the periods during which individual activities or functions are performed, as in a schedule (Gantt or waterfall) chart.

VALIDATION

See CLDP-REQ-1130, Appendix B, Glossary, Validation.

VERIFICATION

See CLDP-REQ-1130, Appendix B, Glossary, Validation.

WHAT WAS REPAIRED

Specific item repaired or replaced to restore functionality.

APPENDIX C - OPEN WORK

Table C-1 lists the specific To Be Determined (TBD) items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBD item is numbered based on the section where the first occurrence of the item is located as the first digit and a consecutive number as the second digit (i.e., <TBD 4-1> is the first undetermined item assigned in Section 4 of the document). As each TBD is solved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above-described numbering scheme. Original TBDs will not be renumbered.

TABLE C-1 TO BE DETERMINED ITEMS

TBD	Section	Description
2-1	2.1	Document not yet baselined.

Table C-2 lists the specific To Be Resolved (TBR) issues in the document that are not yet known. The TBR is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBR issue is numbered based on the section where the first occurrence of the issue is located as the first digit and a consecutive number as the second digit (i.e., <TBR 4-1> is the first unresolved issue assigned in Section 4 of the document). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above-described numbering scheme. Original TBRs will not be renumbered.

TABLE C-2 TO BE RESOLVED ISSUES

TBR	Section	Description

APPENDIX D - METRICS AND MATHEMATICAL MODELS

TABLE D-1 RELIABILITY METRICS AND MODELING

Metric	Description	Mathematical Representation	Focus	Outcome
λ	The total number of failures within the population divided by the total number units of life expended by that population, during a particular measurement interval, under stated conditions.	Used to estimate reliability for items with a constant failure rate: $R(t) = e^{-\lambda t}$	For items that have a constant failure rate (e.g., electronics), the exponential distribution is used to model the mean time between failures, where R represents the reliability for a given duration, t.	Lower λ implies that the system remains operable for a longer duration.
MTBF	The mean number of life units during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions.	$MTBF = \frac{\text{cumulative time}}{\text{number of failures}}$ or $MTBF = \frac{1}{\lambda}$	Informs management about items that may require periodic maintenance (removal, replace, repair, etc.).	Higher MTBF implies system remains operable with less frequent downtime.
Series Model	Assuming a system is composed of n items that are critical to the operation of that system, then the system reliability is the probability that all or n components function correctly.	$R_s(t) = e^{-(\lambda_1 + \lambda_2 + \dots + \lambda_n)t}$ $R_s(t) = \prod_{i=1}^n R_i$	In a series model, all of the components require to be successful for the system to be successful.	System reliability is improved when actions are taken to address the most vulnerable components of the system.

Metric	Description	Mathematical Representation	Focus	Outcome
Parallel Models	Parallel models are used to represent and estimate reliability for redundant systems.	$R_p(t) = 1 - [(1 - e^{-\lambda_1 t})(1 - e^{-\lambda_2 t}) \dots (1 - e^{-\lambda_n t})]$ $R_p(t) = 1 - \prod_{i=1}^n (1 - R_i)$	Model is used to determine the number of redundant components needed to improve the reliability.	Determine the optimum number of redundant components based on how it impacts the design (reliability, complexity, mass, and costs, etc.).
Active Redundancy Model	Redundancy wherein all redundant items are operating simultaneously.	$R_a(t) = \sum_{k=m}^n \left(\frac{n!}{k! (n-k)!} \right) (e^{-\lambda t})^k (1 - e^{-\lambda t})^{(n-k)}$	Model accounts for simultaneous operating redundant items	Reflects the type of redundancy used in the architecture so that the reliability quantitative results reflect the architecture.
Standby Parallel Model	Redundancy wherein the alternative means of performing the function is not operating until it is activated upon failure of the primary mean of performing the function.	$R_{sp}(t) = e^{-\lambda t} \sum_{i=0}^{n-1} \left(\frac{(\lambda t)^i}{i!} \right)$	Model accounts for redundant items that remain dormant until activated.	Reflects the type of redundancy used in the architecture so that the reliability quantitative results reflect the architecture.
Shared Load Parallel Model	Redundancy wherein multiple components are arranged in parallel, meaning they all work together to handle a load, and when one component fails, the remaining components	$R_{sl}(t) = e^{-2\lambda_1 t} + 2\lambda_1 t * e^{-\lambda_2 t}$	Model accounts for parallel redundant items that work together to handle a load where if one item fails the remaining items share the workload.	Reflects the type of redundancy used in the architecture so that the reliability quantitative results reflect the architecture.

Metric	Description	Mathematical Representation	Focus	Outcome
	automatically share its workload			
Bayes' theorem	Bayesian approach uses past experience, knowledge, and learning process to estimate the probability of an event P(A) and when additional information, evidence, or objective data based on testing is available, the previous estimate, P(A), is modified based on the new information, P(A/B).	$P(A B) = P(A) \frac{P(B A)}{P(B)}$ In general: $P(A_i B) = P(A_i) \frac{P(B A_i)}{\sum_{i=1}^k P(A_i) P(B A_i)}$	Used to update the first estimate assuming the new information is valid and appropriately applied.	Used to improve reliability estimations from design through operations.

TABLE D-2 MAINTAINABILITY METRICS

Metric	Description	Mathematical Representation	Focus	Outcome
MTTR	MTTR is the total CM time divided by the number of CM actions performed.	$MTTR = \frac{\sum_{i=1}^n \lambda_i \cdot MTTR_i}{\lambda_i}$	Informs management of the mean downtime for CM during a particular interval under stated conditions.	Lower MTTR implies that the system remains operable for a longer duration.
MTBF	The mean number of life units during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions.	$MTBF = \frac{\text{cumulative time}}{\text{number of failures}}$ or $MTBF = \frac{1}{\lambda}$	Informs management about items that may require periodic maintenance (removal, replace, repair, etc.).	Higher MTBF implies system remains operable with less frequent downtime.

TABLE D-3 AVAILABILITY METRICS

Metric	Description	Mathematical representation	Focus	Outcome
A_i	Inherent availability represents the probability that a system, when used under stated conditions, without consideration for any scheduled or preventive action, in an ideal support environment (available tools, spares, personnel, data, etc.) operates satisfactorily at a given point in time. This excludes preventive maintenance, supply delay, or administrative delay time.	$A_i = \frac{MTBF}{MTBF + MTTR}$	Informs management of the uptime capability accounting for the mean time to repair.	Lower MTTR improves overall uptime capability
A_a	Achieved availability represents the probability that a system or equipment, when used under stated conditions in an ideal support environment (available tools, spares, personnel, data, etc.) operates satisfactorily at	$A_a = \frac{MTBF}{MTBF + MAMT}$ Where, MAMT is the mean active maintenance time, the mean time to perform a corrective or preventive maintenance action.	Informs management of the uptime capability accounting for mean active maintenance time.	Lower MAMT improves overall uptime capability.

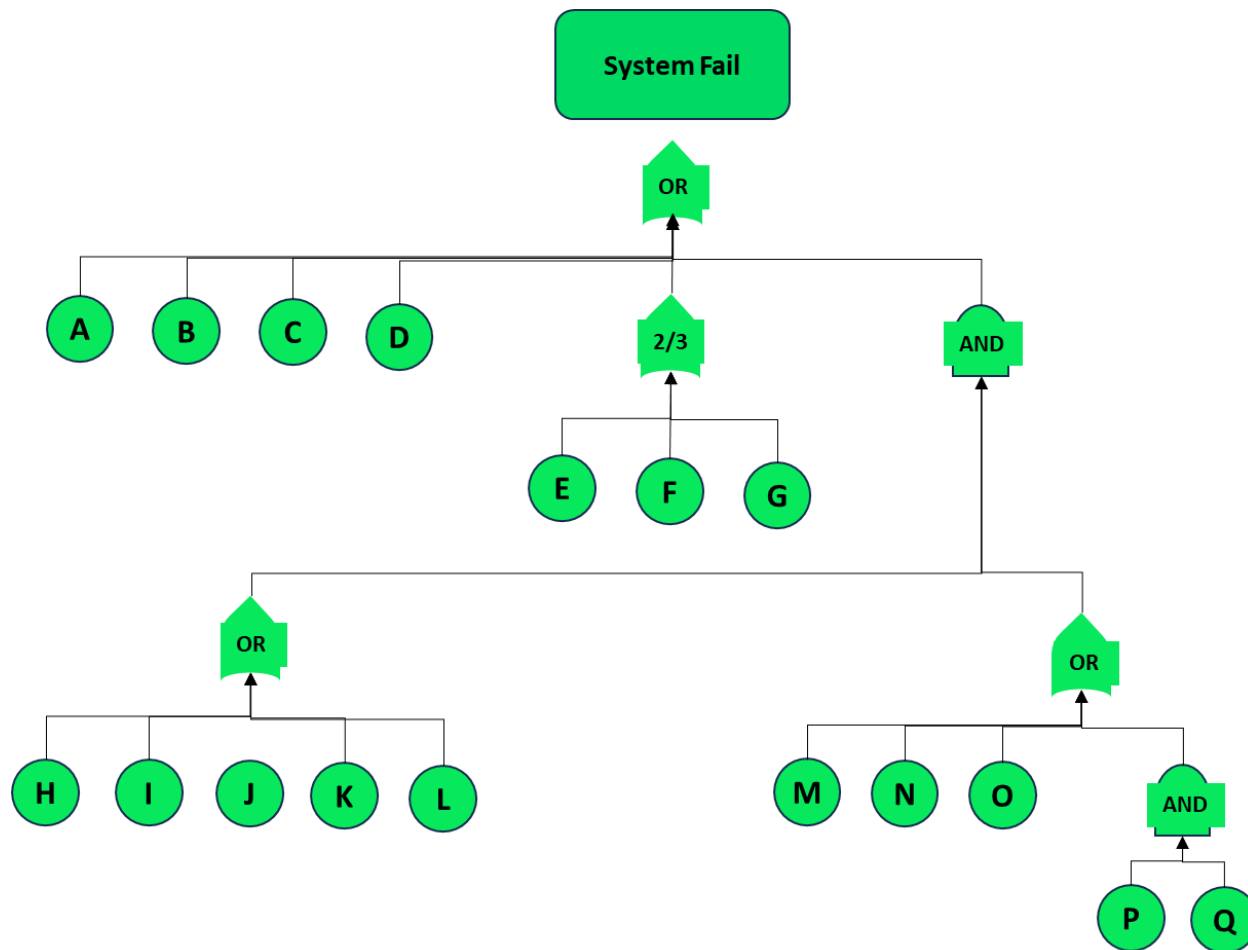
CLDP-PLN-3115
Revision A

Metric	Description	Mathematical representation	Focus	Outcome
	a given point in time. This form of system availability includes both corrective- and preventive-maintenance tasks (but not supply delay and administrative delay times).			
A_o	Operational availability represents the probability that a system or equipment, when used under stated conditions in an actual operational environment, operates satisfactorily at a given point in time. This form of system availability includes the maintenance delays (supply delay and administrative delay).	$A_o = \frac{MTBM}{MTBM + MDT}$ Where, MDT is the mean downtime that accounts for the mean active maintenance time, supply delay time, and the average administrative delay time.	Informs management of the uptime capability accounting for the mean down.	Lower MDT improves overall uptime capability. Note: Operational availability represents what is likely to be seen by the user since it includes the maintenance delays that can be expected to occur in actual operation.

APPENDIX E - MODELING APPROACHES

E.1 FAULT TREE ANALYSIS

Fault Tree Analysis is a systematic, deductive methodology for defining a single specific undesirable event and determining all possible reasons (failures) that could cause the event to occur. The model describes combinations of failure events that can cause a specific system failure of interest (top event). A fault tree uses the top event as a starting point to develop or identify underlying and/or successive causes until basic events (irreducible, root causes) are identified. The causes are arranged in logical order using logical operators or conditions or gates that represent how the top event occurs. Collectively, top event, subsequent events, basics events, arranged in logical arrangement using logical operators, conditions, or gates visually represent a tree. As a reliability model, a fault tree model is constructed/sequenced to represent and/or align with the system architecture. Failure probabilities can then be assigned to the identified failure events to assess the probability of a specific system failure top event.



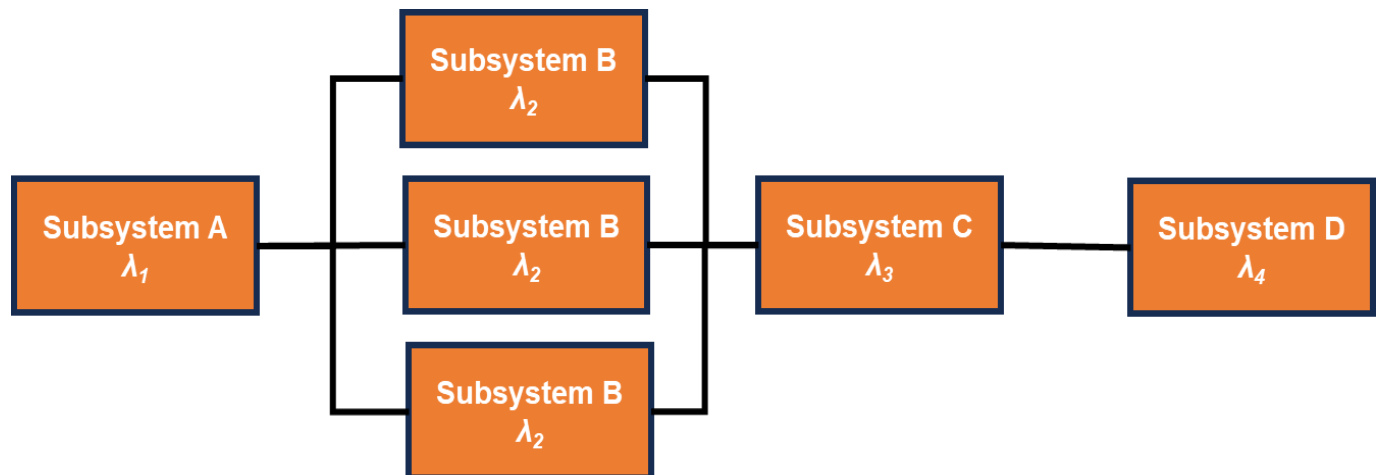
NOTE: This figure is for reference only.

FIGURE E.1-1 FAULT TREE DIAGRAM EXAMPLE

E--1

E.2 RELIABILITY BLOCK DIAGRAM ANALYSIS

Reliability Block Diagram Analysis (RBDA) is a top-down analysis method that represents the organization of the system allowing for functional organization into subsystems. The RBD illustrates the dependence and/or independence of the elements in contributing to the reliability requirements. This diagram yields the effects of the failures on the overall system performance and provides a set of rules that defines the satisfactory or unsatisfactory operation of the system. The RBD allows for parallel, redundant, and standby paths and can be constructed in either a failure or success basis. The RBD is keyed and traceable to the functional block diagram, schematics, and drawings and provides a basis for accurate mathematical representation of reliability. The functional block diagram provides a graphical description of the functions and interrelationships of a system that is then used to build the RBD to ensure an accurate representation of the system.

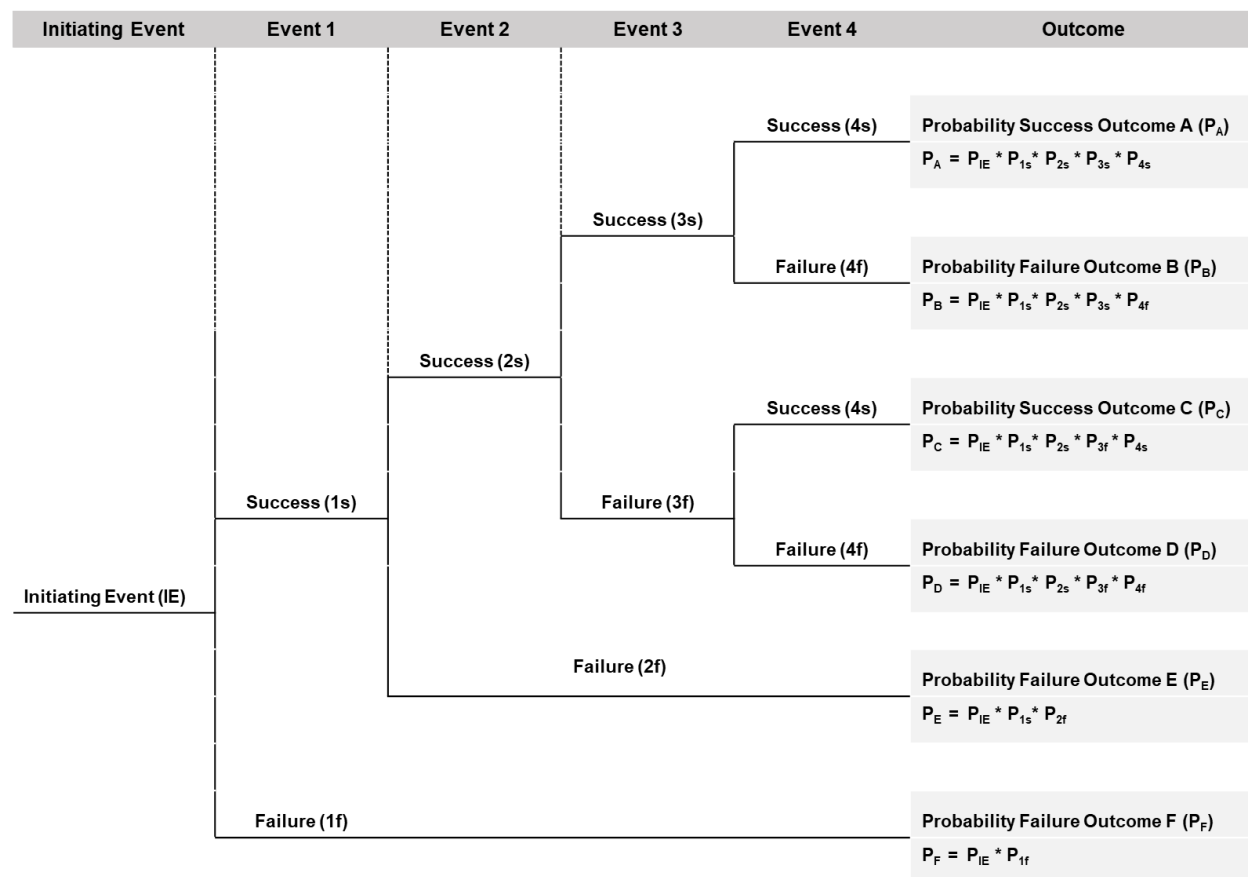


NOTE: This figure is for reference only.

FIGURE E.2-1 RELIABILITY BLOCK DIAGRAM EXAMPLE

E.3 EVENT TREE ANALYSIS

An event tree analysis (ETA) is an analysis model describing a range of potential accident sequences given a specific initiating event. ETA is used to identify a suite of potential outcomes resulting from a specific initiating event and can account for timing, dependence, and domino effects that are cumbersome to model in fault trees. An event tree is developed inductively through a chronological order from the initiating event through intermediate safeguards and conditions, to the ultimate consequence. This model can help determine the control strategy to be applied to reduce the occurrence or eliminate contributing factors that leads to the ultimate consequence.

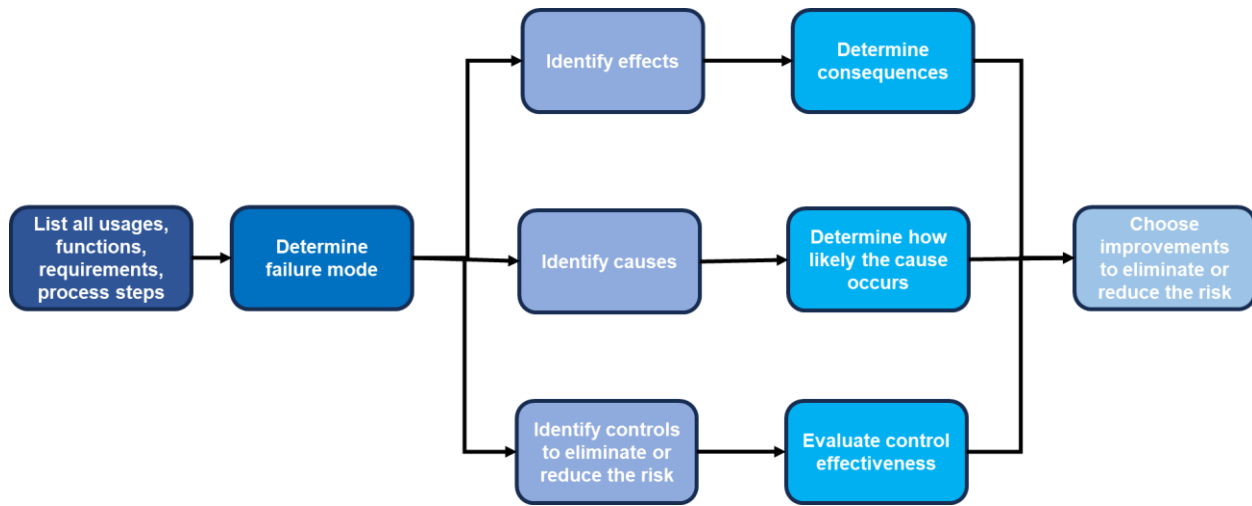


NOTE: This figure is for reference only.

FIGURE E.3-1 EVENT TREE DIAGRAM EXAMPLE

E.4 FAILURE MODES AND EFFECTS ANALYSIS

A failure modes and effects analysis are used to analyze each potential failure mode of an item to determine the results or effects of the item on the system. When analysis is extended to classify each potential failure mode according to its severity and probability of occurrence, a CIL is developed, managed and maintained to show how vulnerabilities revealed by the analysis are addressed.



NOTE: This figure is for reference only.

FIGURE E.4-1 FAILURE MODES AND EFFECTS ANALYSIS METHODOLOGY

TABLE E.4-1 CRITICALITY DEFINITIONS

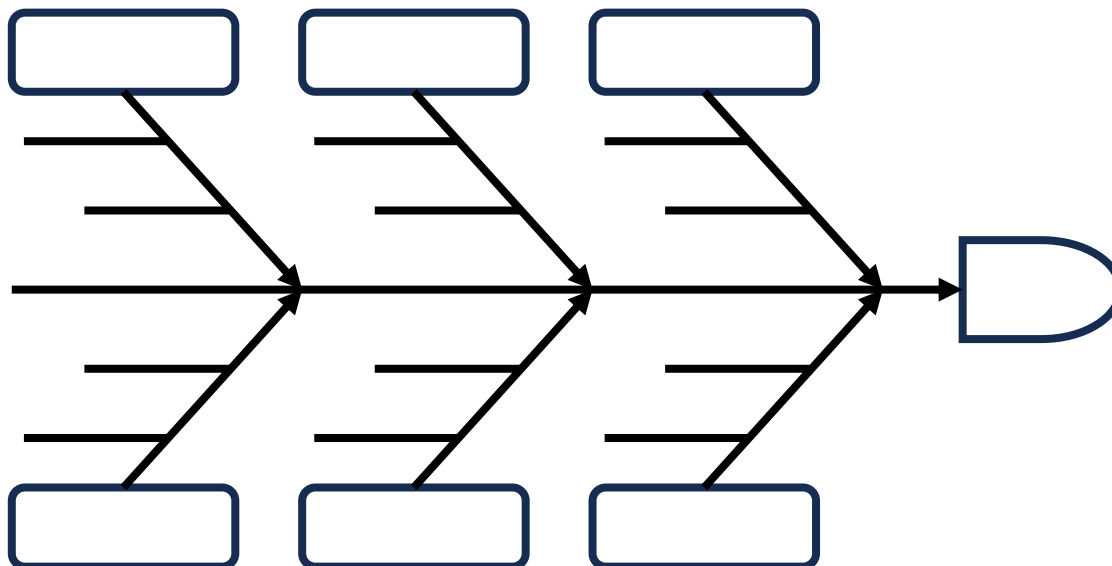
Criticality	Definition (Potential Effect of Failure)
1	Single failure that could result in loss of Space Station, visiting vehicle, or life.
1R	Redundant hardware items, which if all fail, could result in loss of Space Station, visiting vehicle, or life.
1S	Single failure in a safety or hazard monitoring system that could cause the system to fail to detect, combat, or operate when needed during the existence of a catastrophic condition and could result in loss of Space Station, visiting vehicle, or life.
1SR	Redundant hardware items in a safety or hazard monitoring system, which if all fail, could cause the system to fail to detect, combat, or operate when needed during the existence of a catastrophic condition and could result in loss of Space Station, visiting vehicle, or life.
2	Single failure that could result in damage of flight hardware (i.e. ORU).
2R	Redundant hardware items, which if all fail, could result in damage of flight hardware.
3	All others.

TABLE E.4-2 COMMON CAUSE DEFENSE MECHANISMS

Defense Mechanism	Description
Functional Barrier	Modification of the equipment functional interconnections.
Physical Barrier	Physical restriction, barrier, or separation (e.g., watertight door to preclude flooding of an equipment room).
Monitoring/Awareness	Increased monitoring, surveillance, or personnel training.
Maintaining Staff and Scheduling	A maintenance program modification such as staggered testing and maintenance/operation staff diversity.
Component Identification	Identical trains in a system and similar systems in multi-plant facilities. Examples of this would be more visible equipment identification, bar coding, and color-coding.
Diversity	A modification to diversity in equipment, types of equipment, procedures, equipment functions, manufacturers, suppliers, personnel, etc.

E.5 CAUSE AND EFFECT ANALYSIS

Problem-solving technique that involves systematically identifying and investigating the potential causes of a specific issue or problem aiming to understand the relationship between the causes and their resulting effects, ultimately allowing for targeted solutions to be developed [Fishbone Diagram].



NOTE: This figure is for reference only.

FIGURE E.5-1 FISHBONE DIAGRAM TEMPLATE

E.6 PHYSICS OF FAILURE APPROACH

The physics of failure approach to reliability improvement uses detailed knowledge of the expected life-cycle load profile combined with the material properties of key elements of the design to identify potential flaws, reasons for flaw precipitation, and the details of the propagating failure mechanisms that lead to ultimate component failure and system level malfunction. This approach may provide a scientific basis for estimating product life under actual operating conditions and given that the approach starts at an early design stage, identifies key failure mechanisms. Depending upon the physics of the failure, different types of modeling can be employed to represent mechanical, thermal, electrical, etc., stresses that lead to low level component failures. Failure modeling is based on root cause failures with propagation mechanisms. The failure mechanisms need to address the design parameters and variability that are closely tied to a specific reliability concern.

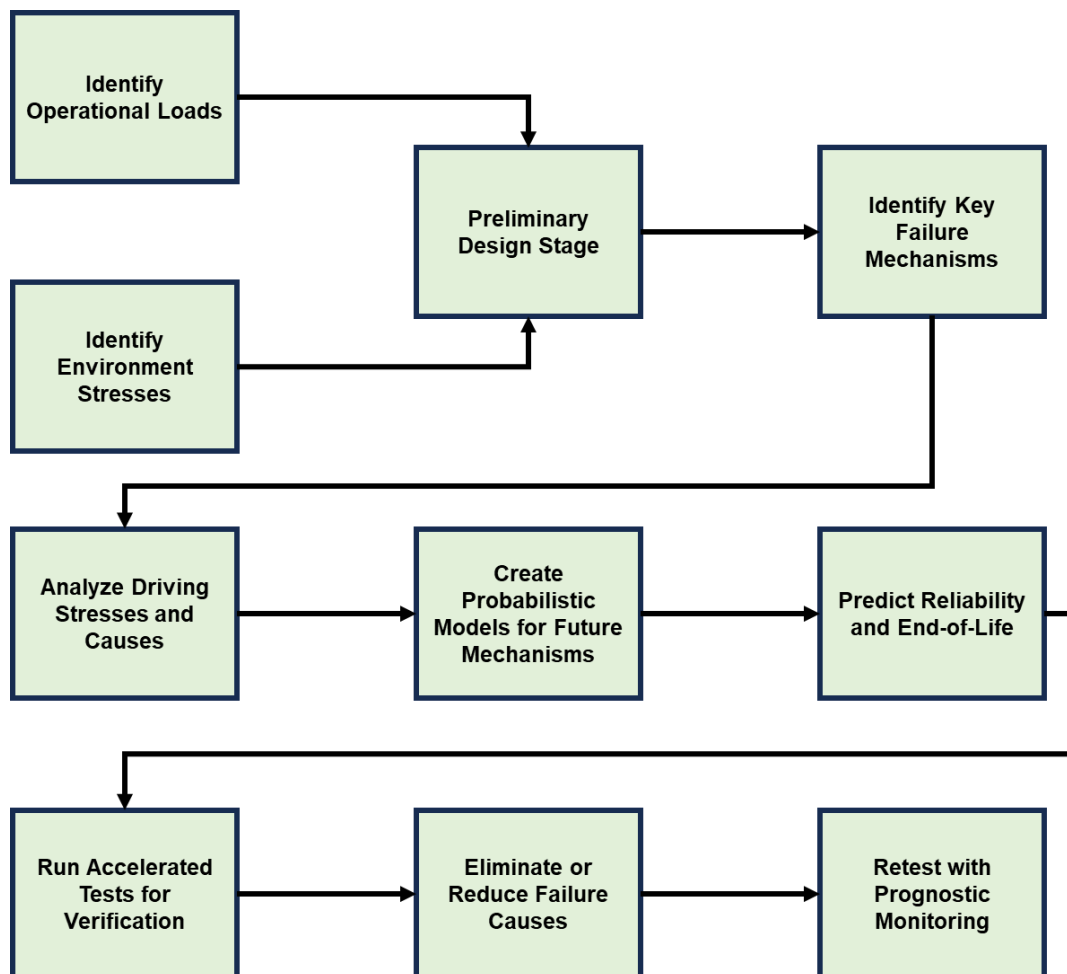


FIGURE E.6-1 PHYSICS OF FAILURE PROCESS IN DESIGN

APPENDIX F - ORBITAL REPLACEMENT UNIT SELECTION PROCESS

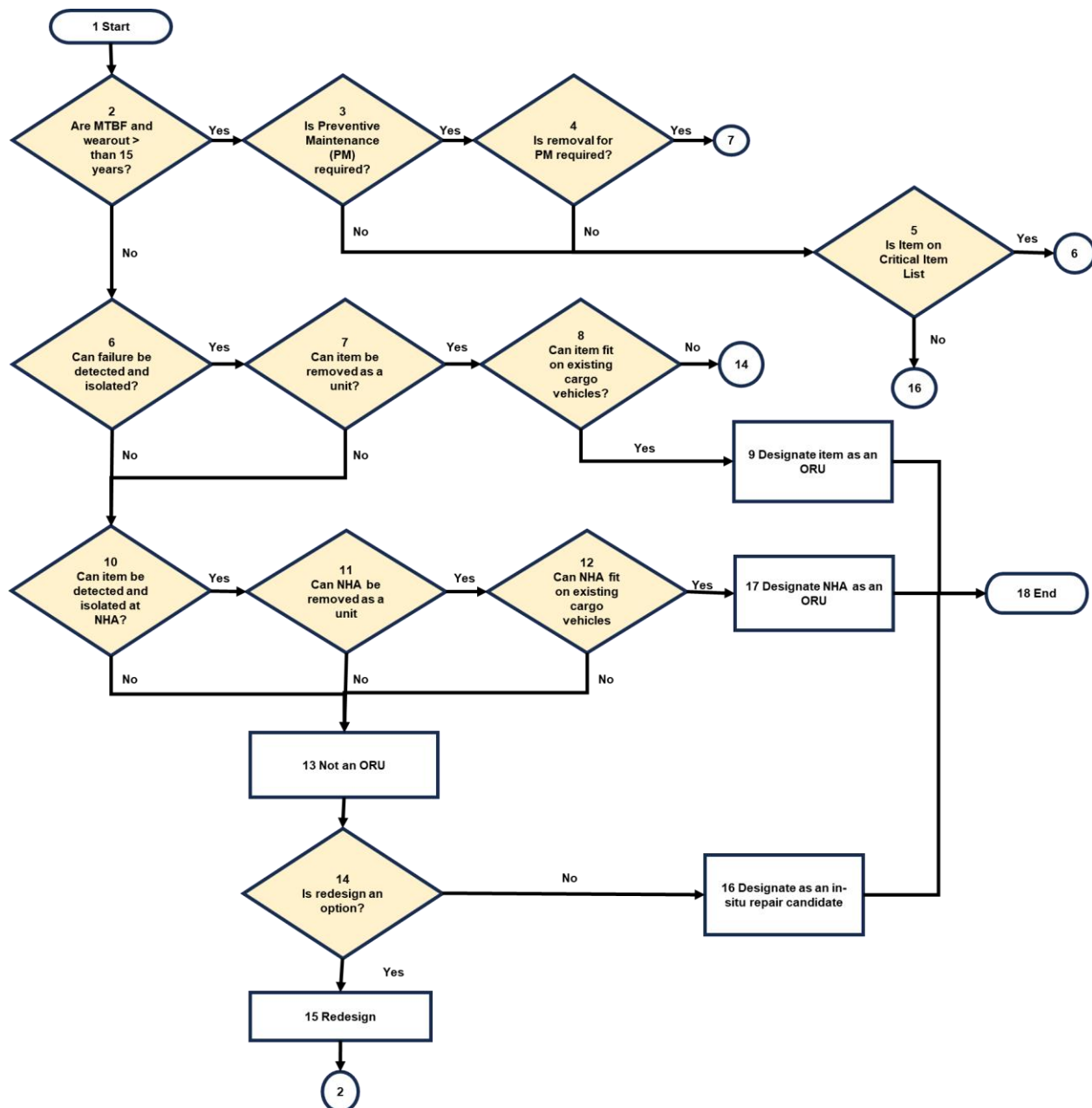


FIGURE F-1 ORBITAL REPLACEMENT UNIT SELECTION PROCESS

The ORU selection process is used to determine which hardware is designated to be capable of being removed and replaced by the on-board crew in accordance with the Maintenance Concept. New hardware being developed is evaluated for suitability as an ORU. Following is a description of each block of the Selection Process. Below is the rationale for each of the blocks.

CLDP-PLN-3115
Revision A

1. Start. Beginning of the ORU selection process
2. Mean Time Between Failure (MTBF) and Wear out > 15 years. This block uses a coarse assessment of the hardware under consideration. The assumption is that any new hardware is intended to operate for 15 years from initial activation. If the total installed population of new hardware has an aggregate inherent failure rate of greater than 15 years, or a wear out factor of greater than 15 years, the item may still need to be an ORU if Preventive Maintenance is required (Block 3). If either of these values are less than 15 years, ORU designation is determined by the ability to fault isolate, remove/replace and resupply the item (Blocks 6-8). If no MTBF or Wear out value has been developed, engineering judgment may be used to determine whether the hardware item can reasonably be expected to exhibit a failure within 15 years to qualify for "no" answer and move decision to block 6. An item with a robust design should not need to undergo Remove and Replace (R&R).
3. Is Preventive Maintenance Required? An assessment of the need for a Preventive Maintenance task (remove/replace, cleaning, etc.) in accordance with Section 9 is used here. A PM requirement does not immediately designate the hardware as an ORU. This is determined in subsequent decision blocks.
4. Is Removal for PM Required? The life limiting factor of the hardware may necessitate its removal to reset the interval. Removal drives tools and procedure which means LSAR. Some PM tasks, such as cleaning or lubrication, may be performed in situ.
5. Is the Item on the Critical Item List? Items that are highly reliable (Block 2) or have no PM requirement (Block 3) may still need to be designated as an ORU. The R&M Working Group is responsible for evaluating the hardware item to determine whether it should be added to the Critical Item List. Critical means you provide Spare and have LSAR even though item is reliable and requires no PM.
6. Can failure be detected by Fault Detection/Fault Isolation (FD/FI)? If a failure of the item can be detected by Built In Test/Built In Test Equipment (BIT/BITE), or if telemetry from the item can be assessed to determine a failure, the Yes Arrow should be followed.
7. Can Item undergo R&R as a Unit? If the item can be removed at the Organizational Level in accordance with the Maintenance Concept (Section 9.0), the Yes Arrow should be followed.
8. Can item fit on existing cargo vehicles? In order for a remove/replace maintenance concept to be viable, the replacement item needs to be transportable on the current fleet of cargo vehicles. If the item cannot fit on an existing cargo vehicle a redesign needs to be considered.
9. Designate Item as an ORU. ORU selection is complete.
10. Can Item be FD/FI at the Next Higher Assembly (NHA)? In the event that the item under consideration cannot meet the need for FD/FI (same as Block 6), the NHA

CLDP-PLN-3115
Revision A

may be considered for selection as an ORU. This block is also satisfied if FD/FI can be accomplished with either BIT/BITE or assessment of telemetry.

11. Can NHA be removed as an assembly? If the NHA can meet the need for FD/FI, then it needs to be assessed for removal as a unit (same as Block 7).
12. Can NHA fit on existing cargo vehicles? In order for a remove/replace maintenance concept to be viable, the replacement item needs to be transportable on the current fleet of cargo vehicles. If the item cannot fit on an existing cargo vehicle a redesign needs to be considered.
13. Not an ORU. Arriving at this block indicates that the hardware item needs to be maintainable due to its expected reliability, but the current design does not support the ability to remove/replace and resupply the item. Therefore, redesign is necessary.
14. Is redesign an option? Redesign may not be possible if the required functionality cannot be repackaged to meet the constraints of the installation footprint and cargo resupply. The option to redesign may also not be feasible due to cost or schedule constraints. If redesign is feasible, proceed to Block 15. If not, proceed to Block 16.
15. Redesign. Design change to accommodate the constraints of the installation footprint and cargo resupply.
16. Designate as an in-situ repair candidate. In this instance, the hardware item has to be maintained in its installed location. In situ repair tasks include alternate routing of interconnecting devices (e.g., cables and fluid lines, rather than replacement when alternative routing is significantly more efficient than replacement) or performance of light structural repairs to include straightening, fluid line repair, and connector repair.
17. Designate NHA as an ORU. ORU selection is complete.
18. End. End of the ORU selection process.