



CLDP-STD-3102
Baseline

Commercial Low-Earth Orbit Development Program (CLDP) Hazard Analysis and Safety Process Standard

Baseline

August 2025

DRAFT

This document has been approved for public release via the Scientific, Technical and Research Information DiscoVEry System (STRIVES) 20250008716 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
Baseline	Initial Release (Reference Directive CLDP-DXXXX, EFF. XX-XX-XX) Program Release	XX-XX-XXXX
DRAFT		

PREFACE

**COMMERCIAL LOW-EARTH ORBIT DEVELOPMENT PROGRAM (CLDP) HAZARD
ANALYSIS AND SAFETY PROCESS STANDARD**

The contents of this document are intended to be consistent with the tasks and products to be prepared by the Commercial LEO Development Program Providers. This document is under the control of a Joint Program Control Board (JPCB) with CLDP and Commercial Crew Program (CCP). The JPCB is the authority for baselining and approving changes. This document was developed and is maintained by the CLDP Safety and Mission Assurance (S&MA) Office.

DRAFT

Angela T. Hart
Program Manager
Commercial Low-Earth Orbit Development Program

Date

Joseph "Steve" Stich
Program Manager
Commercial Crew Program

Date

COMMERCIAL LOW-EARTH ORBIT DEVELOPMENT PROGRAM (CLDP)
HAZARD ANALYSIS AND SAFETY PROCESS STANDARD
CONCURRENCE
AUGUST 2025

Prepared by:	<u>Andrea Monsalve-Garvey</u>	<u>US</u>
	CLDP BOOK MANAGER	ORG
	<u><i>Andrea Monsalve-Garvey</i></u>	<u>8/07/2025</u>
	SIGNATURE	DATE
Prepared by:	<u>Felisha Drake-Hill</u>	<u>OP111</u>
	BOOK COORDINATOR/DQA	ORG
	<u><i>Felisha Drake-Hill</i></u>	<u>8/07/2025</u>
	SIGNATURE	DATE
Concurred by:	<u>Jenny Andrews</u>	<u>US</u>
	MANAGER, SAFETY & MISSION ASSURANCE OFFICE	ORG
	<u><i>Jay E. Andrews</i></u>	<u>8/07/2025</u>
	SIGNATURE	DATE

TABLE OF CONTENTS

PARAGRAPH	PAGE
1.0 INTRODUCTION.....	1-4
1.1 PURPOSE.....	1-4
1.2 SCOPE.....	1-4
1.3 CHANGE AUTHORITY/RESPONSIBILITY.....	1-4
1.4 PRECEDENCE	1-4
1.5 VERB APPLICATION.....	1-4
2.0 DOCUMENT	2-1
2.1 APPLICABLE DOCUMENTS	2-1
2.2 REFERENCE DOCUMENTS	2-1
3.0 HAZARD ANALYSIS OVERVIEW.....	3-1
3.1 HAZARD SEVERITIES/LIKELIHOOD	3-1
3.1.1 HAZARD CONTROL STRATEGY.....	3-3
3.1.2 DESIGN FOR MINIMUM RISK	3-3
3.1.3 FAILURE TOLERANCE	3-4
3.1.3.1 FAILURE TOLERANCE FOR CRITICAL HAZARDS	3-4
3.1.3.2 FAILURE TOLERANCE FOR CATASTROPHIC HAZARDS.....	3-5
3.1.3.3 FAILURE TOLERANCE AND EMERGENCY SYSTEMS.....	3-5
3.1.4 PROCESS CONTROLS.....	3-5
3.1.5 EMERGENCY RESPONSE	3-6
3.1.5.1 CREW SURVIVAL METHODS.....	3-6
3.1.5.2 DESTINATION SURVIVAL METHODS.....	3-7
3.1.6 COMPUTER SYSTEM SAFETY	3-8
3.1.7 COMPUTER-BASED CONTROL SYSTEM	3-9
3.1.8 HAZARDOUS MATERIAL CONTROL STRATEGY	3-10
3.1.8.1 TOXIC MATERIALS.....	3-10
3.1.8.2 BIOLOGICAL MATERIALS	3-11
3.1.8.3 FLAMMABLE MATERIALS	3-13
3.1.8.4 ECLSS HARDWARE AND CABIN ENVIRONMENTAL IMPACT.....	3-14
3.1.8.5 PHYSICAL AGENTS.....	3-16
3.1.8.6 RADIOACTIVE MATERIALS.....	3-17
3.1.8.7 HAZARD RESPONSE LEVELS.....	3-17
3.2 HAZARD CONTROL ORDER OF PRECEDENCE	3-19
3.3 SAFETY NON-COMPLIANCE/VARIANCE	3-19
3.3.1 SAFETY NON-COMPLIANCE/VARIANCE DOCUMENTATION.....	3-19
3.3.2 EQUIVALENT SAFETY NON-COMPLIANCE/VARIANCE.....	3-20
3.3.3 PROGRAM LEVEL NON-COMPLIANCE/VARIANCE.....	3-22
3.3.4 EFFECTIVITY OF NON-COMPLIANCES/VARIANCE	3-23
4.0 SAFETY HAZARD ANALYSIS DEVELOPMENT AND SAFETY MILESTONES.....	4-1
4.1 SAFETY DOCUMENTATION.....	4-2
4.1.1 SDP DOCUMENTATION STRATEGIES.....	4-2
4.1.2 HAZARD REPORTS	4-2

CLDP-STD-3102
Baseline - DRAFT

4.1.2.1	HR STRUCTURE	4-3
4.1.3	TECHNICAL DATA SUPPORTING HAZARD ANALYSIS	4-9
4.2	SAFETY MILESTONES	4-21
4.2.1	PHASE 0 – CONCEPT DEVELOPMENT	4-25
4.2.2	PHASE I – PRELIMINARY DESIGN	4-25
4.2.3	PHASE II – FINAL DESIGN	4-26
4.2.4	PHASE III – FINAL ACCEPTANCE	4-26
4.2.5	FLIGHT SAFETY CERTIFICATE	4-27
4.2.6	VERIFICATION CLOSEOUT	4-27
4.2.7	SAFETY VERIFICATION TRACKING	4-28
4.2.8	POST-PHASE III ACTIVITIES	4-28
4.2.8.1	POST-PHASE III (PRIOR TO FLIGHT) SAFETY APPROVAL	4-29
4.2.8.2	POST-FLIGHT SAFETY APPROVAL	4-29
4.2.8.3	ON-ORBIT RECONFIGURATION	4-29
4.2.8.4	MISSION UNIQUE HAZARDS	4-30
4.3	SERIES, REFLOWN, AND MODIFIED HARDWARE	4-30
5.0	SAFETY REVIEW ROLES AND RESPONSIBILITIES	5-1

APPENDIX

APPENDIX A	ACRONYMS AND ABBREVIATIONS	A-1
APPENDIX B	GLOSSARY	B-1
APPENDIX C	OPEN WORK	C-1
APPENDIX D	BEST PRACTICES FOR HAZARD ANALYSIS TYPES	D-1
APPENDIX E	BEST PRACTICES FOR SAFETY DATA DEVELOPMENT	E-1
APPENDIX F	BEST PRACTICES FOR PHASED SAFETY REVIEWS	F-1
APPENDIX G	BEST PRACTICES FOR SAFETY REVIEWS ROLES AND RESPONSIBILITIES	G-1
APPENDIX H	GOVERNMENT FURNISHED SERVICES TRANSPORTATION	H-1
APPENDIX I	IMPORTANT NASA/NESC MEMOS	I-1
APPENDIX J	COMMENTS DOCUMENTATION	J-1
APPENDIX K	BEST PRACTICES FOR GROUND SAFETY	K-1
APPENDIX L	DFMR CONTROL APPROACH GUIDANCE	L-1
APPENDIX M	BEST PRACTICE EXPECTATIONS – NASA SEVEN ELEMENTS OF FLIGHT RATIONALE	M-1

TABLE

TABLE 3.1-2	HAZARD LIKELIHOOD DEFINITIONS	3-3
TABLE 3.1.8.1-1	TOXICITY HAZARD LEVEL (THL) AND HAZARD SEVERITY (2 PAGES)	3-11
TABLE 3.1.8.2-1	NASA IN-FLIGHT BIOSAFETY LEVEL RATING AND HAZARD SEVERITY	3-12
TABLE 3.1.8.3-1	FLAMMABILITY HAZARD LEVEL AND HAZARD SEVERITY	3-13
TABLE 3.1.8.4-1	ECLSS HARDWARE IMPACT RATING (E RATING) AND HAZARD SEVERITY	3-15
TABLE 3.1.8.4-2	ECLSS CABIN ENVIRONMENTAL IMPACT RATING	3-16
TABLE 3.1.8.5-1	PHYSICAL AGENTS AND HAZARD SEVERITY	3-17
TABLE 3.1.8.7-1	LEVELS OF CONTROL AND HAZARD RATINGS	3-18
TABLE 3.3.2-1	EQUIVALENT SAFETY CONSIDERATIONS/CRITERIA (2 PAGES)	3-21
TABLE 4.1.2-1	LEVELS OF MATURITY	4-3

CLDP-STD-3102
Baseline - DRAFT

TABLE 4.1.2.1-1	HAZARD REPORT DATA (3 PAGES).....	4-3
TABLE 4.1.2.1-3	HAZARD REPORT DATA – CONTROLS (2 PAGES).....	4-6
TABLE 4.1.2.1-4	HAZARD REPORT DATA – VERIFICATIONS (3 PAGES)	4-7
TABLE 4.1.3-1:	TECHNICAL DATA SUPPORTING HAZARD ANALYSIS (11 PAGES)	4-10
TABLE 4.2-1	SAFETY MILESTONES AND DEVELOPMENT SCHEDULE (3 PAGES).....	4-22
TABLE C-1	TO BE DETERMINED ITEMS	C-1
TABLE C-2	TO BE RESOLVED ISSUES	C-1
TABLE D.2-1	HAZARD ANALYSIS TYPES.....	D-2
TABLE D.2.1.1-1	PHL WORKSHEET SAMPLE INSTRUCTIONS	D-7
TABLE D.2.1.6-1	O&SHA FORMAT AND DATA ELEMENTS.....	D-11
TABLE D.2.1.9.1-1	RESPONSIBILITY MATRIX.....	D-15
TABLE D.3-1	ELEVATED RISK ACCEPTANCE REPORTING.....	D-17
TABLE D.3-2	HAZARD SCORING MATRIX EXAMPLE.....	D-17
TABLE G.1-1	MISSION PHASE SAFETY REVIEW ROLES AND RESPONSIBILITIES	G-1
TABLE I.1-1	POLICY MEMOS/TECHNICAL REQUIREMENTS INTERPRETATION LETTERS (2 PAGES).....	I-1
TABLE L.1-1:	ISS EXAMPLE DFMR LIST (4 PAGES)	L-1

FIGURE

FIGURE D.3.31-1	HAZARDOUS MATERIAL SUMMARY TABLE.....	26
FIGURE J.1-1	BATTERY DESCRIPTION FORM	2
FIGURE K.1.1-1	EXAMPLES OF COMMENT FORM	1
FIGURE K.1.2-1	COMMENTS EXAMPLE.....	2

1.0 INTRODUCTION

1.1 PURPOSE

This document establishes minimum standards for Hazard Analysis (HA) processes and methodologies for the Commercial Low-Earth Orbit (LEO) Development Program (CLDP) to promote a comprehensive and accurate safety analytical practices to identify and document all hazards, hazard controls, crew survivability approaches, and emergency response methods. It also communicates best practices and lessons learned from the National Aeronautics and Space Administration (NASA).

1.2 SCOPE

This document applies to the Commercial LEO Destination System (CLDS), Utilization, and associated activities that impact the safety of U.S. Government (USG) crew. The document encompasses the hazard analysis process requirements for safe and successful human space flight missions. Requirements and regulations levied and managed by other government entities are not contained within this document.

1.3 CHANGE AUTHORITY/RESPONSIBILITY

Proposed changes to this document will be submitted by a CLDP Change Request (CR) for consideration and disposition. All changes to this document require the approval of the CLDP Program Control Board (PCB) and CCP PCB.

All such requests will adhere to the CLDP Change Review Process documented in CLDP-P-4010, Commercial Low Earth Orbit Development Program Change Management Process.

The appropriate NASA Office of Primary Responsibility (OPR) identified for this document is CLDP S&MA.

1.4 PRECEDENCE

Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained. In the event of a conflict between this document and the requirements contained within CLDP-REQ-1130, Requirements and Standards for Commercial Low Earth Orbit Development Program, CLDP-REQ-1130 shall take precedence.

1.5 VERB APPLICATION

The following definitions for the implementation of requirement verbs is as follows:

- a) "Shall" – Used to indicate a requirement that is binding, which must be implemented, and its implementation verified in the design or in program documents.
- b) "Should" – Used to indicate good practice or a goal which is desirable but not mandatory.
- c) "May" – Used to indicate permission.

CLDP-STD-3102
Baseline - DRAFT

- d) “Will” – Used to indicate a statement of fact or declaration of purpose on the part of the government that is reflective of decisions or realities that exist and are to be taken as a given and not open to debate or discussion.
- e) “Is” or “Are” – Used to indicate descriptive material.

Rationales, included for many of the requirements, are intended to provide clarification, justification, purpose, and/or the source of a requirement. If there is an inconsistency between a requirement and its rationale, the requirement always takes precedence.

2.0 DOCUMENT

The documents in Sections 2.1, Applicable Documents, and 2.2, Reference Documents, that are not released will remain <TBD 2-1> until they are baselined.

2.1 APPLICABLE DOCUMENTS

The following documents include specifications, models, standards, guidelines, handbooks, and other special publications. The 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 Section 1.4 of this document.

Document Number	Title
CLDP-P-4010	Commercial Low Earth Orbit Development Program Change Management Process
CLDP-REQ-1130	Requirements and Standards for Commercial Low Earth Orbit Development Program
CLDP-STD-1150	Commercial Low-Earth Orbit Development Program Operations Standards

2.2 REFERENCE DOCUMENTS

The following documents contain supplemental information to guide the user in the application of this document. These reference documents may or may not be specifically cited within the text of this document.

Document Number	Title
ANSI Z136.1	American National Standard for Safe Use of Lasers
CCT-REF-1131	CCT-REQ-1130 Requirement Interpretation Letters
CLDP-PLN-2000	Commercial Low-Earth Orbit Destination System Certification Plan
CLDP-PLN-3016	Commercial Low-Earth Orbit Development Program Insight Management Plan
CLDP-PLN-3017	Commercial Low-Earth Orbit Development Program Utilization Integration Plan
CLDP-PLN-3100	Commercial Low-Earth Orbit Development Program Safety and Mission Assurance Plan
CSD-10000	Human-Rating Requirements for Space Systems

CLDP-STD-3102
Baseline - DRAFT

FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
KNPR 8715.3	KSC Safety Procedural Requirements
JPR 1800.5	Biosafety Review Board Operations and Requirements
JSC 20793	Crewed Space Vehicle Battery Safety Requirements
JSC 26895	Guidelines for Assessing the Toxic Hazard of Spacecraft Chemicals and Test Materials
JSC 62809	Human Rated Spacecraft Pyrotechnic Specification
JSC 65828	Structural Design Requirements and Factors of Safety for Spaceflight Hardware
JSC 66869	Guidelines for the Assessment of Chemicals and Materials for Impacts to Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft
JSC 64825	Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials
NASA-HDBK-2203	NASA Software Engineering and Assurance Handbook
NASA-STD-5017	Design and Development Requirements for Mechanisms
NASA-STD-5019	Fracture Control Requirements for Spaceflight Hardware
NASA-STD-6016	Standard Materials and Processes Requirements for Spacecraft
NASA-STD-7012	Leak Test Requirements
NASA-STD-8739.8	NASA Software Assurance and Software Safety Standard
NESC-IB-24-01986	Failure-Tolerant Avionics for Crewed Space Systems Recommended Best Practices
NPR 2810.1	Security of Information and Information Technology
NPR 7150.2	NASA Software Engineering Requirements

3.0 HAZARD ANALYSIS OVERVIEW

This section, along with its subsequent subsections, establishes core methodologies for performing HAs, stipulates the requirements for documenting those analyses, and outlines the process for accepting the hazard risk for all lifecycle phases and aspects of the CLDS.

A HA of the design and operational concepts is used as a design tool to anticipate and prevent hazardous circumstances that may potentially result in mishaps.

A HA is performed to identify and document all safety hazards, including integrated hazards, technical safety requirements, hazard causes (identifying likelihood and severity), controls (evaluating all hazards for means of eliminating, reducing, or controlling the associated risk), verification methods (test, analysis, inspection, demonstration, etc.), verification closure evidence, hazard risk assessment, crew survival capabilities, and emergency response procedures. It is a systematic process for gaining and evaluating specific information pertaining to the safety of a system and addressing failures that affect government personnel and Utilization.

For each end item, the Commercial Provider shall, from design concept through operational end of life, implement a HA process that includes identifying hazards and risks and controlling and eliminating the hazards to acceptable levels. The Commercial Provider shall, for each hazard, describe compliance to Failure Tolerance (FT) requirements and document the specific approach for this hazard in the HA (reference Section 3.1.2, Failure Tolerance).

The Commercial Provider shall implement configuration management of their HA products, including the Safety Data Package (SDP), Hazard Reports (HRs), and other resulting safety deliverables from their HA under a formal configuration management process, before submission for Phase I review. The Commercial Provider shall also maintain traceability between the operational HA and operational products to related operations and supporting information.

Appendix D.2, Hazard Analysis Types, provides methodologies and examples to document traditional safety analysis techniques.

3.1 HAZARD SEVERITIES/LIKELIHOOD

The Commercial Provider shall categorize hazard risks using the hazard severity levels (Marginal, Critical, and Catastrophic), hazard likelihood levels, and elevated risk acceptance to document the ratings in the hazard scoring matrix to ensure the design meets acceptable residual risks. Hazard severity and likelihood levels are defined in Table 3.1-1, Hazard Severity Definitions, and Table 3.1-2, Hazard Likelihood Definitions.

Elevated risk acceptance reporting is defined in Table D.3-1, Elevated Risk Acceptance Reporting.

Table D.3-2, Hazard Scoring Matrix Example, provides a sample hazard scoring matrix based on the likelihood and severity levels.

Hazard severity level quantifies the worst-case accident or undesired event resulting from a cause without consideration of controls.

TABLE 3.1-1 HAZARD SEVERITY DEFINITIONS

Description		Hazard Severity Definitions
Marginal	Minor	Minor injury not requiring first aid treatment, minor discomfort
	Moderate	Injury requiring first aid treatment, moderate discomfort
	Severe	Injury or occupational illness requiring medical treatment
Critical		Injury or occupational illness that requires medical intervention from a second crewmember and/or Flight Surgeon and is not treatable by first aid alone
Catastrophic		Loss of life or permanently disabling injury

Hazard likelihood is the probability that an identified hazardous effect will occur from the identified hazard cause based on control implementation. Likelihood justification is summarized as rationale for classification of the likelihood, and include assumptions, any empirical data, a qualitative summary of the failure history, and any uncertainties, confidence factors, or limitations (including applicable waivers/deviations/exceptions) in the controls identified in the report that provide the basis for establishing the likelihood or probability of the hazardous event occurring.

When a certain cause(s) is classified with a higher or lower likelihood relative to the other causes within the Hazard Report, additional rationale is necessary to support that classification.

- Marginal Hazards – See Appendix B, Glossary, for definition.
 - Examples of minor crew injuries nominally associated with the marginal severity could include but are not limited to crew discomfort, abrasions, bruises, or superficial burns. Marginal hazards are typically addressed via the Commercial Provider's internal processes and practices. To document a comprehensive HA, the Commercial Provider should summarize/reference the results of their analysis within the associated SDP. Marginal hazards do not require submission of HRs for formal approval.
- Critical Hazards – See Appendix B, Glossary, for definition.
 - Critical hazards are from hardware/software failures that can result in the loss of a major end item, loss of redundancy (i.e., with only a single hazard control remaining) for on-orbit life sustaining function or loss of an emergency system, or loss of use of systems needed for essential logistics or damage to a vehicle or a ground facility occurs. Critical hazards require submission of HRs for formal approval.

- Catastrophic Hazards – See Appendix B, Glossary, for definition.
 - Catastrophic hazards are from hardware/software failures that can result in loss of life (flight crew, ground crew, public) or permanent disabling injury, or an event resulting in the loss of a crew return vehicle. Catastrophic hazards require submission of HRs for formal approval.

TABLE 3.1-2 HAZARD LIKELIHOOD DEFINITIONS

LIKELIHOOD	CRITERIA
Very High	Will occur more than several times or highly likely to occur frequently in the life of the program (Controls are missing or insufficient).
High	Will occur once or likely to occur several times in the life of the program (Controls have significant limitations or uncertainty).
Moderate	Likely to occur sometime in the life of the program (Controls exist, with some limitations or uncertainty).
Low	Unlikely, but possible to occur in the life of the program (Controls have minor limitations or uncertainty).
Very Low	So unlikely, it can be assumed occurrence may not be experienced in the life of the program (Strong controls in place).

3.1.1 HAZARD CONTROL STRATEGY

A hazard control strategy is used to minimize risk of exposure to hazards where hazard controls are used to eliminate or control the hazard cause. Subsequent sections will describe methods or approaches to eliminate or control the hazard cause.

3.1.2 DESIGN FOR MINIMUM RISK

Where failure tolerance is unachievable or impractical, a DFMR approach is permitted for well-understood designs that use proven, verifiable design concepts, analysis, and manufacturing processes. The DFMR approach for designs is based on demonstrated experience and its ability to eliminate or reduce the likelihood of credible failures, instituted by using technical standards and processes, and robust design practices that incorporate design margins to accommodate uncertainties and assure the system is more resilient to credible failures. Design margin is the difference between the required minimum functional capability in the intended operating environment and actual capability. The design margin is intended to accommodate uncertainties and reduce the probability of hazardous events by making the system more resilient to potential failures based on the capability of the material, the operating environment, and their known variability. DFMR approach requires that adequate attention is applied to the design, manufacturing, test, analysis, and inspection of the hardware. The DFMR approach relies on design features and/or flight experience such as years of proven capability, robust design, standard approach, and first-time quality.

The DFMR approach has historically been applied to primary and secondary structures, structural failure of pressure vessels, structural failure of pressurized lines, material

compatibility, and flammability where failure modes are understood and controlled using approved standards and margins for designs with known material properties, capability, variability within a well-defined operating environment.

DFMR is typically a resource intensive effort requiring NASA multidisciplinary review of numerous provider and sub-vendor data sets. Due to the resource-intensive nature of DFMR, it is an option that should be used sparingly, and identified early in the safety process so NASA can adequately arrange for the appropriate subject matter experts to participate in the process.

All candidates for DFMR shall be identified early in the Concept Development phase through the Preliminary Design phase, documented in the PHA and/or HR, and coordinated, reviewed and approved as part of the SDP. Appendix L, DFMR Control Approach Guidance, provides information on DFMR best practices from other NASA programs.

Other potentially catastrophic hazards that cannot be fully controlled using FT and/or DFMR are considered non-compliant and follow the process in Section 3.3, Safety Non-Compliance/Variance.

3.1.3 FAILURE TOLERANCE

Failure Tolerance (FT) is the ability of the design and its operation to continue to safely operate in the presence of a failure(s) and/or operator error(s). The design capability to tolerate the number of failure events and/or operator errors is based on the hazard severity level (critical or catastrophic). The HA and supporting analysis are used to determine the design capability to tolerate various failure events and/or operator errors based on the acceptability of the residual safety risk that is characterized and justified within the HA.

Common cause/mode failures or events can affect multiple controls, inhibits or design features in the system. When redundancy is provided by identical components, locations, or channels, susceptibility to common cause/mode failures may be increased, thereby defeating the intended level of redundancy.

FT shall be evaluated for susceptibility to a common cause/mode event. If susceptible, a design change shall be implemented to eliminate or minimize the susceptibility, and, if susceptibility cannot be eliminated or minimized, provide the technical basis (or rationale) for why the FT susceptibility is acceptable. FT shall assess where dissimilar redundancy reduces safety risk.

3.1.3.1 FAILURE TOLERANCE FOR CRITICAL HAZARDS

Compliance with FT requirements in CLDP-REQ-1130 is accomplished at the end item level or through a combination of hazard controls at the Module/System levels and end item level. To be considered single FT, the HR shall include at least two adequate controls, with valid/appropriate verifications, such that a single failure does not result in a critical hazard for the end item.

3.1.3.2 FAILURE TOLERANCE FOR CATASTROPHIC HAZARDS

Compliance with FT requirements in CLDP-REQ-1130 is accomplished at the end item level or through a combination of hazard controls at the Module/System levels and end item level. To be considered two FT, the HR shall include at least three adequate controls, with valid/appropriate verifications, such that two failures do not result in a catastrophic hazard for the end item.

3.1.3.3 FAILURE TOLERANCE AND EMERGENCY SYSTEMS

Emergency systems and emergency operations cannot be used as a part of FT as these emergency systems and equipment cannot prevent an initiating event. Therefore, a FT strategy without the use of emergency systems or emergency operations will control catastrophic and critical hazards. However, to prevent loss of crew and/or loss of Vehicle/Destination in the event all other approved hazard controls have failed, the use of emergency systems and contingency or emergency operations will be considered an emergency response and/or Crew Survival Methods (CSMs).

After two failures have occurred, evacuation of the Destination is acceptable as a third control to hazards whose only catastrophic effect is loss of crew.

FT requirements apply to ensure that hazards introduced by the presence of the emergency system are identified and controlled. For all such scenarios, the appropriate level of FT, as determined by the integrated design and safety analysis, will be incorporated into the design.

FT requirements do not apply to emergency systems when the systems are activated to perform their intended functions for crew survival. However, design solutions must be in place to ensure the emergency system operates successfully and with high reliability. Emergency system reliability is evaluated to ensure that the emergency system will perform its function as required. This will be deemed adequate through an integrated design analysis that verifies compliance with the design specification for the specific emergency system. Where applicable, that integrated design analysis will meet any reliability allocation requirements for the emergency system.

3.1.4 PROCESS CONTROLS

Process controls used in manufacturing, assembly, test, handling, or transportation processes are crucial in assuring reliable design controls (i.e., FT or DFMR) to control and manage risk of exposure to hazards. Control and mitigation of such hazard causes will be based on process controls (e.g., critical manufacturing, cleanliness standards, materials selection, procurement standards and processes, parts control programs, quality management systems, etc.), which are typically the only method of controlling and preventing the hazard cause. Examples of hazard controls that require process controls include improper design, improper material selection, contamination of item causes failure, etc.

The Commercial Provider shall identify the process-based hazard controls in the HR and provide, as part of the SDP, identification of the controlling standards or requirements that govern the process, the methods by which the process is controlled

and verified to conform to those governing standards, and, if non-conformances exist, the technical basis or rationale for acceptance.

3.1.5 EMERGENCY RESPONSE

Emergency response methods **<TBR 3-1>** include the use of emergency equipment and systems used to contain hazards that have occurred which present an immediate threat to:

- a. The crew
- b. Crewed Destination, Crew Visiting Vehicle (CVV) or Cargo Visiting Vehicle (CaVV) during integrated operations
- c. Efforts to save the crew (through Crew Survival Methods), and,
- d. Efforts to save the Destination (through Destination Survival Methods).

The end goal is to interrupt the progress of the hazardous event and/or provide a means to isolate, mitigate, and/or control hazards.

At a minimum, the Commercial Provider shall perform a HA, develop, and document for emergency systems and deliver to the appropriate safety review board, by including the following:

- a. Evaluation of an emergency system during dormant/non-use state:
 - Assessment when the system is in the non-operational or non-emergency operational state during a nominal mission. Assessment includes potential effects and hazardous conditions introduced by the presence of the emergency system on the nominal operations of the vehicle.
 - Assessment of the failures of the emergency system that could lead to a hazard. This includes inadvertent or accidental operation of the system, i.e., “must not work”.
- b. Evaluation of the emergency response actions/procedures during use state:
 - Assessment of hazardous substance release (gas, liquid, particulate), depress, fire, loss of attitude control, and medical emergencies.
 - Verification that the crew has been trained in the use of emergency response actions/procedures.

Appendix D.4.1, Emergency Response Procedures, and D.4.1.1, Emergency Response Equipment and Systems, contains additional HA guidance on emergency response procedures, equipment, and systems.

3.1.5.1 CREW SURVIVAL METHODS

Crew survival is defined as the capability and ability to preclude crew/passenger fatality or permanent disability. This will include the use of a suite of emergency response capabilities. CSMs represent the total set of requirements, analyses, equipment,

training, and procedures used to isolate, mitigate and/or control exposure to an imminent catastrophic condition that presents an immediate threat to the crew. Crew survivability also considers response when emergency systems have failed and may, for example, consider such actions as reduced survival mode until crew rescue or crew return can be attempted.

The Crew Survival Summary details the incorporation of system capabilities to implement crew survival strategies for each phase of the reference missions. It includes:

- a) The system failures and emergencies (such as fire, collision, toxic atmosphere, decreasing atmospheric pressure, and medical emergencies) with specific capabilities (such as abort, safe haven, rescue, emergency egress, emergency systems, and emergency medical equipment or access to emergency medical care) identified to protect the crew.
- b) The effectiveness of crew survival capabilities under conditions and time constraints to be encountered during high-risk accident conditions and their impact on the risk to the crew.
- c) How the survival capabilities will be maintained during the scenarios.
- d) The implementation of the survival capabilities identified and clear traceability to the highest-level program documentation.

The Commercial Provider shall identify applicable CSMs, and develop and document crew survival analysis, in each catastrophic hazard cause within an HR, by including the following:

- a. CSM scenarios and analysis including a description of chain of events that leads to an imminent threat to crew (e.g., external events, system failures) including emergency events (i.e., fire, collision, toxic release, depressurization, and medical emergencies),
- b. Designed and operational capabilities that protect the crew (such as abort, safe haven, rescue, emergency egress, emergency systems, and emergency medical equipment or access to emergency medical care),
- c. Crew roles, responsibilities, and involvement.

The Commercial Provider can identify capabilities for their specific design that enhance crew survival including those required by CLDP-REQ-1130. Identifying CSMs (and Emergency Response Methods) for each catastrophic hazard cause increases the probability of crew survival in the presence of imminent catastrophic conditions.

Appendix D.4.1.2, Crew Survival Methods, provides additional guidelines for crew survival documentation.

3.1.5.2 DESTINATION SURVIVAL METHODS

Destination survival methods represent the total set of requirements, analyses, equipment, training, and procedures intended to secure the safety of the Destination after a potentially catastrophic event sequence has started. While no NASA requirements are levied on the Destination to provide for its recovery and/or survivability

after the occurrence of a hazardous event, NASA expects that the Commercial Providers will want the ability to preserve their Destination in the event of a potentially catastrophic event (hazardous substance release, micro meteoroid orbital debris strike resulting in depress, fire, etc.)

The Commercial Provider should document any identified destination survival methods. The Commercial Provider shall document destination survival methods in the HRs and SDP and require NASA approval if USG Crew is involved in the destination survival methods-specific response or the risk to USG Crew is increased during the response.

3.1.6 COMPUTER SYSTEM SAFETY

In typical vehicle designs, the capabilities needed to perform critical functions are predominantly implemented in flight software.

The HA process shall:

- a. Assess the specific avionics and software architecture sensitivity to software malfunctions (Appendix D.5, Computer System Safety, contains a list of standard types of malfunctions).
- b. Identify the time-to-detect (TTD) of a software malfunction.
 - This ensures that any planned recovery can be implemented between TTD and time-to-effect (TTE) timeframe.
- c. Identify the TTE of each applicable hazard.
 - This determines if the software can be recovered or repaired before a catastrophic hazard is realized.
- d. For each type of malfunction, identify, evaluate, and address common cause/mode failures within the operational scenarios and mission phases.

Appendix D.5, Computer System Safety, contains a list of examples of common cause/mode failures and software common cause/mode failures.

The Commercial Provider shall identify and summarize relevant software discrepancies, problem reports or non-conformances, in which these discrepancies, problems, and failures can be traced in the SDP (Failure Mode and Effects Analysis (FMEA), fault tree, control, or verification compromise).

A Black Out Zone (BOZ) is a flight phase in which hazard controls and mitigations do not provide sufficient time to prevent a catastrophic event. The software BOZ analysis identifies areas where a software common cause/mode failure could cause a catastrophic hazard, does not meet the failure tolerance requirement and will need risk acceptance. Historically, BOZ analysis successfully served as a hazard verification for software common cause/mode failure cause analysis.

A primary mechanism for minimizing the risk of common cause/mode failure and providing the primary control in hazard space is through stringent development processes, which ensures software/avionics designs are robust, with considerations for safety critical software. This activity begins with developing software in accordance with

meeting levied requirements in CLDP-REQ-1130, industry standards, and best practices to prevent the introduction of individual faults, which may eventually manifest as common cause/mode failures.

Appendix D.5.1, Black Out Zone Analysis, contains further BOZ analysis guidance.

Appendix D.5.2, Common Cause/Mode Failure Control Strategy and Risk Mitigations, contains additional guidance on capturing common cause/mode failure control strategies and risk mitigations.

3.1.7 COMPUTER-BASED CONTROL SYSTEM

Computer-Based Control System (CBCS) requirements are applied to systems with computer or complex electronic control that control a safety-critical process or device and whose inadvertent operation, or failure, can result in a critical or catastrophic hazard. To minimize risks associated with the use of computers, the hazard control is developed using engineering and management principles, criteria/standards, and techniques to tolerate hardware failures and software errors.

The Commercial Provider shall perform the following:

- a. Identify any safety-critical subsystems that are computer controlled via the CBCS
- b. Identify the CBCS architecture, software description, and final CBCS system design associated with that computer control, and
- c. Classify each system and subsystem containing software as prescribed by NPR 7150.2, NASA Procedural Requirements NASA Software Engineering Requirements.

As part of the SDP, the Commercial Provider shall deliver the following:

- a. Software safety data as prescribed by NASA-STD-8739.8B, NASA Technical Standard Software Assurance and Software Safety Standard.
- b. CBCS Safety Assessment, which details CBCS compliance to CLDP-REQ-1130 requirements, identifies safe states and control paths, evaluates Must Work functions (MWF) and Must Not Work Functions (MNWFs) along with their transitions, and provides a list of hazardous commands
- c. Trace between software safety requirements and software system hazards, controls, conditions, and events
- d. Safety analysis of off-the-shelf and reused software
- e. Any documentation or analysis in support of CBCS in hazard space

Specific detail and requirements for hazard areas utilizing CBCS are provided in CLDP-REQ-1130.

Reference Section 3.0, Hazard Analysis Overview, for HA methodologies and Appendix D.5.4, Software Safety Hazard Analysis, for further guidance on the Software Safety HA process.

3.1.8 HAZARDOUS MATERIAL CONTROL STRATEGY

The Commercial Provider shall develop and utilize a hazardous material control strategy that:

- a. Describes the process, methods, tools, and roles and responsibilities for identifying, assessing, documenting, approving, and communicating information related to hazardous materials and the hazards controls for both design, development, test and evaluation and real time operations.
- b. Defines the classifications, hazardous material hazard levels, hazard severity levels, and Hazard Response Levels (HRLs) for hazardous materials.
- c. Provides the identified level of controls to prevent the inadvertent or uncontrolled release of hazardous materials

While potential hazards and their control strategy should be considered during the selection of materials, the above process is applicable after material selection is completed per CLDP-REQ-1130.

Hazardous materials that do not have a credible path into the pressurized habitable environment are not included in the hazard assessment.

Hazardous material hazard levels and corresponding hazard severity levels are defined in Sections 3.1.8.1 to 3.1.8.7.

HRLs are defined in Section 3.1.8.7 and Table 3.1.8.7-1.

The Provider shall include the information in Appendix D.6.1, Hazardous Material Summary Table, in the SDP and to crew and operators during real time operations **<TBR 3-2>**. Appendix D.6.1 defines the information that is captured in a Hazardous Material Summary Table (HMST) and the specific information and maturity that is expected to be communicated during the Phased Safety Reviews and real-time operations. An HMST is a NASA example of how to document and communicate hazardous material information.

3.1.8.1 TOXIC MATERIALS

Toxicity Hazard Level (THL) and hazard severity are defined in Table 3.1.8.1-1.

The THL addresses all chemicals and potential chemically induced toxicity hazards are assessed and provided a THL. This applies to all chemicals that may be located, used, or introduced into the pressurized habitable environment and encompasses all physical states and compositions (for example: solid, liquid, vapor, gas, gel, grease, and powders/particulates) for chemicals and potential products of end item chemical reactions. Materials can be classified as organic, inorganic, polymeric, biological, radioactive, acidic, basic, neutral, oxidants, hypertonic or hypotonic. These chemical, physical and/or biological properties, together with their intrinsic toxicity, flammability, and biohazard potential, determine the hazard level of the materials.

THL 4 compounds can pose an immediate risk to crew health and can cause permanent injury. These compounds are not containable once released, cannot be cleaned up by the crew and may not be scrubbed from the environment by the Environmental Control and Life Support System (ECLSS) system.

The THL of a mixture of chemicals is determined from the toxicity of the entire mixture or, if not known, the most toxic component in that mixture. If there is little or missing information for a chemical (for example, Commercial-Off-The-Shelf (COTS) items), the THL rating will be conservative to ensure safe conditions.

TABLE 3.1.8.1-1 TOXICITY HAZARD LEVEL (THL) AND HAZARD SEVERITY (2 PAGES)

Hazard Severity	THL	Description
Marginal	0	Any gas, gel, solid, or liquid that has the potential for, at worst, short-term, slight chemical (i.e. not mechanical) irritation that will not require therapy
Critical	1	Any gas, gel, solid, or liquid that has the potential for slight to moderate irritation that will not resolve quickly (in <30 minutes) without intervention
Catastrophic	2	A containable solid, gel, or non-volatile liquid that has the potential for moderate to severe irritation and/or ocular damage that may have a long-term performance impact
	3	A containable solid or low-volatility liquid that has the potential for appreciable systemic effects, long-term serious injury (e.g. cancer), or internal tissue damage
Not Allowed	3 decomposing to 4	A containable solid or low-volatility liquid that has the potential for appreciable systemic effects, long-term serious injury (e.g. cancer), or internal tissue damage that decomposes to an uncontainable gas, volatile liquid, or fine particles/fume that has the potential for moderate to severe irritation, and/or appreciable systemic effects, and/or a long-term performance impact
	4	An uncontainable gas, volatile liquid, or fine particles/fume that has the potential for moderate to severe irritation, and/or appreciable systemic effects, and/or a long-term performance impact
Material offgassing, sometimes referred to as toxic offgassing, is generally not assessed under THL hazard ratings, but may be assessed in special cases where material offgassing is expected to occur during operations, such as 3-D printing. Description developed by the JSC Toxicology and Environmental Chemistry Group based on JSC 26895, Guidelines for Assessing the Toxic Hazard of Spacecraft Chemicals and Test Materials.		

Note: The NASA SMACs and the American Conference of Governmental Industrial Hygienists (ACGIH) Threshold Limit Values (TLVs) indicate maximum concentrations of exposure to airborne contaminants (i.e. vapors). The SMACs, TLVs, and THLs are based on different criteria and are meant to be used in very different circumstances so there is no direct quantitative relationship between them.

3.1.8.2 BIOLOGICAL MATERIALS

Biosafety Level (BSL) and hazard severity are defined in Table 3.1.8.2-1.

All biological material and potential biohazards are assessed and provided a BSL. This applies to vectors of biological materials such as animals and plants, non-biological materials such as soil or dust, and environmental conditions such as warm, moist air that may harbor or promote the growth of biological materials.

Biosafety Levels are established to protect the crew and environment from immediate or latent biohazards, including contamination of food and water supplies. Due to the typically nonvolatile nature, biological materials do not impact the ECLSS impact hazard ratings. Factors that affect the BSL rating include the origin and volume of the biological material, physical state of the sample growth medium (solid or liquid), infectivity dose, medical or spacecraft integrity consequences, and proposed operations/usage.

If there is limited information available on a biological material or the operation and use, the BSL rating may be elevated to ensure safe conditions on the vehicle. When two or more biohazardous materials or agents are present in an end item, the hazard severity will be driven by the highest BSL rating.

Due to microgravity conditions in space, aerosols from microorganisms can be more of a risk factor than on Earth as larger particles and droplets can be suspended as aerosols for longer timeframes. In consideration of microgravity, the BSL-2 category is divided into BSL-2M (Moderate) and BSL-2H (High).

TABLE 3.1.8.2-1 NASA IN-FLIGHT BIOSAFETY LEVEL RATING AND HAZARD SEVERITY

Hazard Severity	NASA Biosafety Level (BSL) Rating	Description
Marginal	1	Well-characterized agents not known to consistently cause diseases in healthy adults, minimal hazard to environment
Critical	2M (Moderate)	Moderate risk agents associated with human disease. Primary exposure routes include skin (percutaneous) exposure, ingestion, and mucous membrane exposure.
Catastrophic	2H (High)	Higher risk agents associated with human disease. Risk is increased by lower infectious dose, likelihood of aerosolization, larger amounts of agent presents and other factors
Not Allowed*	3	Agents with potential for airborne transmission. May cause life-threatening diseases.
	4	Agents with high potential for life threatening disease. High potential for aerosol transmission of agent with no disease prevention (prophylactic) or specific therapy
<i>Description developed in coordination with NASA/JSC Biosafety Review Board based on JPR 1800.5, Biosafety Review Board Operations and Requirements.</i> NOTE: The In-Flight BSL is commonly referred to as BSL instead of In-Flight BSL * BSL 3 and 4 are prohibited from use on Destinations		

Appendix D.6.2, Biological Materials, contains historical examples of BSL ratings.

3.1.8.3 FLAMMABLE MATERIALS

Flammability Hazard Level (FHL) and hazard severity are defined in Table 3.1.8.3-1.

The FHL addresses all chemicals that are flammability hazards. Spacecraft fire control is based on minimizing potential ignition sources and eliminating materials that can propagate fire. Controlling the quantity and configuration of flammable materials to eliminate potential fire propagation paths ensures that any fire would be small, localized, isolated, and would self-extinguish without harm to the crew. The FHL of a mixture of chemicals is determined from the flammability of the entire mixture or the most flammable component in that mixture depending on the chemical components.

TABLE 3.1.8.3-1 FLAMMABILITY HAZARD LEVEL AND HAZARD SEVERITY

Hazard Severity	FHL	Description	Flash Point*	
			Temperature °F (°C)	Volume (ml)
Acceptable (Not a hazard)	0	Any liquid, powder or gas considered to be a nonflammable material and limited quantities of flammable liquids and powders based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of < 20 liters	< 120 (49)	< 5
			120 (49) – 200 (93)	< 25
			200 (93) – 300 (148)	< 50
			> 300 (148)	<250
Critical	1	Flammable liquid, powder and gas; quantity limits for liquid and powder are based on the flammable material's flash point Flammable gas quantity is limited based on gas cloud production of 20-100 liters	< 120 (49)	5 – 25
			120 (49) – 200 (93)	25 – 100
			200 (93) – 300 (148)	50 – 250
			> 300 (148)	250 – 1000
Catastrophic	2	Flammable liquids and powders; quantity limits are based on the flammable material's flash point	< 120 (49)	25 – 100
			120 (49) – 200 (93)	100 – 250
			200 (93) – 300 (148)	250 – 500
			> 300 (148)	> 1000
	3	Flammable liquids and powders; quantity limits are based on the flammable material's flash point	< 120 (49)	100 – 250
			120 (49) – 200 (93)	250 – 500
			200 (93) – 300 (148)	500 – 1000
			> 300 (148)	
	4	Flammable liquid, powder and gas; quantity limits for liquid and powder are based on the flammable material's flash point	< 120 (49)	> 250
			120 (49) – 200 (93)	> 500
			200 (93) – 300 (148)	> 1000

Hazard Severity	FHL	Description	Flash Point*	
		Flammable gas quantity is limited based on gas cloud production of ≥ 100 liters	> 300 (148)	
Description details developed in coordination with NASA/JSC Materials and Processes Branch based on JSC 64825A, Guidelines for Assessing the Flammability Hazard of Spacecraft Chemicals and Test Materials.				
* The flash point is the lowest temperature at which a chemical can form vapors or an ignitable mixture in the air that will ignite given an ignition source. A lower flash point is an indication that the chemical is easier to ignite.				

3.1.8.4 ECLSS HARDWARE AND CABIN ENVIRONMENTAL IMPACT

The ECLSS Hardware Impact Rating (E Rating) and hazard severity are defined in Table 3.1.8.4-1.

ECLSS Hardware Impact Rating (E Ratings, scale: E0 to E6) addresses the impacts of exposure to chemicals or physical agents on ECLSS resources, consumables, and the rated service life of the system and/or essential components of the system. These ratings are based on release of the chemical into the vehicle and it assumes complete failure of the controls that prevent release of the chemical.

Appendix D.6.3, ECLSS Hardware and Cabin Environmental Impact, contains an explanation on ECLSS E Rating and THL relationship.

TABLE 3.1.8.4-1 ECLSS HARDWARE IMPACT RATING (E RATING) AND HAZARD SEVERITY

Hazard Severity	ECLSS Hardware Impact Rating (E Rating)	Description
Acceptable (Not a hazard)	E0	No ECLSS performance degradation. No change in scheduled maintenance. (Operational capacity* consumption is <2%, with 100% of the capacity margin** retained.)
	E1	No ECLSS performance degradation. No change in scheduled maintenance. (Operational capacity consumption is >2% and <10%, with > 10% of the capacity margin consumed.)
Marginal	E2	ECLSS functional performance is degraded by <10%. Early replacement of consumable components may be necessary within nine months. (Operational capacity consumption is >10% and <25%, with > 25% of the capacity margin consumed.)
	E3	ECLSS functional performance is degraded by >10% and <25%. Early replacement of consumable components may be necessary within six months. (Operational capacity consumption is >25% and <50%, with > 50% of the capacity margin consumed.)
Critical	E4	ECLSS functional performance is degraded by >25% and <50%. Early replacement of consumable components may be necessary within one month. (Operational capacity consumption is >50% and <75%, with > 75% of the capacity margin consumed.)
	E5	ECLSS functional performance is degraded by >50% and <75%. System maintenance is required to restore functional performance within one week. (Operational capacity consumption is >75% and <90%, with 100% of the capacity margin consumed.)
	E6	ECLSS functional performance is degraded by >75%. System maintenance is required to restore functional performance within one day. (Operational capacity consumption is >90%, with >100% of the capacity margin consumed.)
Description details developed in coordination with NASA/ISS ECLSS Engineering Group based on JSC 66869, Guidelines for the Assessment of Chemicals and Materials for Impacts to Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft. * Operational capacity: capability of the system performance ** Capacity margin: allowance provided for system performance (hardware is nominally operated at less than 100% to allow for margin)		

ECLSS Cabin Environmental Ratings are defined in Table 3.1.8.4-2.

ECLSS Cabin Environmental Impact Rating (scale: A to E) addresses the ability of ECLSS to recover the cabin atmosphere to acceptable levels when hazardous material is released. This rating is an indicator of how long the chemical may persist in the cabin environment and depends upon the chemical and the ECLSS hardware's ability to remove the chemical from the cabin environment. Maintaining and/or recovering the cabin atmosphere is taken into consideration with the final assigned THL. The ratings do not directly correlate to hazard severity; however, they are a consideration for crew exposure and determination of THL ratings.

TABLE 3.1.8.4-2 ECLSS CABIN ENVIRONMENTAL IMPACT RATING

ECLSS Cabin Environmental Impact Rating	Time for ECLSS to Reduce Contamination Concentration by 95%*
A	0-2 hours
B	2-24 hours
C	24-72 hours (1-3 days)
D	72-168 hours (3-7 days)
E	> 168 hours (7 days) ECLSS is unable to remove chemical and it persists in the environment
Details developed in coordination with NASA/ISS ECLSS Engineering Group based on JSC 66869, Guidelines for the Assessment of Chemicals and Materials for Impacts to Environmental Control and Life Support Systems and Habitable Volumes of Crewed Spacecraft.	
* Acceptable level for crewmember to breathe without protective filtration masks	

3.1.8.5 PHYSICAL AGENTS

Physical Agents severity levels are defined in Table 3.1.8.5-1. Physical agents are not rated under a scaled hazard rating but are classified based on potential release and hazard severity.

Table 3.1.8.5-1 is provided based on specific particle density, lung deposition, and minute volume; the concentration limit will differ for different minute volumes or particle densities. The routine or purposeful release of particles should be identified when the end item data is provided for review as indicated in the verifications. As particles addressed here are considered physiological hazards instead of chemically induced toxicity hazards, a THL rating is not assigned. Instead, the details will be captured in the end item's HMST as a note in the comments section.

This category encompasses particles and fluids that are in the habitable volume and act as physical agents when released.

Particles that are determined to be chemically inert and/or insoluble in water are a nuisance at low concentrations and a physical hazard at high concentrations. The concentrations identified in Table 3.1.8.5-1 apply to short duration events driven by failures that would release particles rapidly. It does not apply to a routine or intermittent source of particles or over long periods of time. For these particles and use, hazard control measures to limit exposures should be implemented. For example, nanoparticle

generation by routine three-dimensional (3D) printing should be controlled to prevent release or limit release to acceptable levels.

Appendix D.6.4, Physical Agents, contains more information on physiological and shatterable material hazards due to particle release.

TABLE 3.1.8.5-1 PHYSICAL AGENTS AND HAZARD SEVERITY

Type of Physical Agent	Not a Hazard	Hazard Severity		
	Acceptable Level	Marginal	Critical	Catastrophic
Inert, Insoluble Particle				
Size of particle > 10 µm	$C \leq 10 \text{ mg/m}^3$	N/A	$10 \text{ mg/m}^3 < C < 50 \text{ g/m}^3$	$C \geq 50 \text{ g/m}^3$
Size of particle ≤ 10 µm	$C \leq 3 \text{ mg/m}^3$	N/A	$3 \text{ mg/m}^3 < C < 13 \text{ g/m}^3$	$C \geq 13 \text{ g/m}^3^*$
Inert, Insoluble Particle				
Sharp Particles	$PS \leq 50 \text{ µm}^{**}$	N/A	N/A	$PS > 50 \text{ µm}$
Non-Sharp Particles	$PS \geq 500 \text{ µm}^{**}$	N/A	$PS < 500 \text{ µm}^{**}$	$C \geq 50 \text{ g/m}^3$
Table is based on NASA/ JSC Toxicology and Environmental Chemistry Group and TOX-VR-2023-01 NASA/JSC Space Medicine Particle Policy. C = concentration; R = release; PS = particle size * Concentration limit will vary based on minute volumes and particle density. The value identified here assumes a particle density of 1.5 g/cc, 50% deposition in the lungs, and a minute volume of 10 liters/min during an exposure duration of about 360 minutes, divided by a safety factor of 2. ** Particles of this size may present a potentially catastrophic hazard if released at high velocity.				

3.1.8.6 RADIOACTIVE MATERIALS

All radioactive material/radiation producing equipment (e.g., radioactive isotopes, X-ray devices) are classified as a catastrophic hazard. Accordingly, the primary radioactive material/radiation producing equipment or source of radiation is controlled to prevent release through failure tolerance and to ensure compliance with the crew exposure limits. The necessity and utilization of radioactive material in end items should be carefully reviewed and the radiation source material should be kept As Low As Reasonably Achievable (ALARA). For example, if radioactive material is used to calibrate equipment, it should be a radiation source that produces the lowest amount of radiation to achieve the required result.

3.1.8.7 HAZARD RESPONSE LEVELS

HRLs are defined in Table 3.1.8.7-1.

HRLs identify the immediate actions required to protect the crew in response to a spill or leakage of a particular hazardous material on orbit. It reflects the minimum for post-spill safety clean-up and does not necessarily reflect the level of control required for the end item design. The HRL is an integrated response rating determined by the most severe rating for toxicity, biosafety, and flammability hazards associated with a particular hazardous material or grouping of hazardous materials.

CLDP-STD-3102
Baseline - DRAFT

The level of control is based on the hazard severity level for hazardous materials in the worst-case environment. The hazardous materials are assessed and assigned specific hazard ratings based on the type of hazardous material and potential hazards to the crew, the habitable environment and/or equipment. Hazard ratings are scaled to define the potential risk and hazard severity for the release of hazardous materials without regard to controls.

Table 3.1.8.7-1 defines the relationship between levels of control and the hazardous material hazard ratings.

TABLE 3.1.8.7-1 LEVELS OF CONTROL AND HAZARD RATINGS

HRL	Hazard Severity	Level of Control Amount	THL	BSL	FHL	ECLSS Hardware Impact Rating (E-Rating)
0 (Green)	Not a Hazard	0 Level of Control			0	E0-E1
	Marginal Hazard	1 Level of Control	0	1		E2-E3
1 (Blue)	Critical Hazard	2 Levels of Control	1	2 (Mod)	1	E4-E6
2 (Yellow)	Catastrophic Hazard	3 Levels of Control	2	2 (High)	2, 3, 4	
3 (Orange)			3			

Notes:

- [1] HRL (color indicated in table) is an indication for the integrated on-orbit response for THL, BSL and FHL; HRL reflects the minimum for post-spill safety clean-up and does not necessarily reflect the level of containment/control required for the end item design
- [2] Level of controls are assessed by NASA as part of the safety review process
- [3] Controls for Marginal Hazards are summarized/referenced within the associated SDP
- [4] THL 2-3, BSL-2H, and FHL 2-4 all require 3 Levels of control
- [5] THL 4 (and THL 3 decomposing to 4) are not allowed
- [6] Varying level of control for FHLs are based on hazardous material properties/quantities in the end item
- [7] E-Ratings are included to show the relationship to level of control and are not part of the HRL
- [8] Levels of control for physical agents are also based on the hazard severity
- [9] The flammability hazard level of a liquid is determined by a combination of the flash point and volume of that liquid and is based upon the assumption that the entire volume of liquid is spilled. For gases, the flammability hazard level determined on a case-by-case basis.

[10] While FHL of the substance does not drive a need for Personal Protective Equipment (PPE), FHL 2-4 require at least 2 levels of containment for clean-up, and therefore are designated HRL1.

3.2 HAZARD CONTROL ORDER OF PRECEDENCE

Most hazards will require the combination of these approaches to adequately control a potential hazard.

1. Eliminate the hazard.
2. Reduce the risk (severity and/or likelihood) through design alteration.
3. Use of Operational Controls.

Appendix D.7, Hazard Control Order of Precedence, contains a detailed description of each hazard control strategy and hazardous effect mitigation strategies.

3.3 SAFETY NON-COMPLIANCE/VARIANCE

End item design or operations that do not comply with an applicable safety requirement require a Non-Compliance/Variance and efforts should be taken to bring the end item into compliance. The Commercial Provider shall document non-compliances in the appropriate HR and notify NASA upon identification.

A Safety Non-Compliance/Variance is categorized as one of the following two types: Equivalent Safety (ES) Non-Compliance/Variance and Program Level Non-Compliance/Variance. Approval of a Non-Compliance/Variance for the end item design or operation will not relieve the Commercial Provider of the responsibility to meet the requirement in any other module, subsystem, or component of other end items.

For end items with a non-compliant condition, additional rigor and scrutiny may be required to validate hazard controls, risk mitigations, and acceptance rationale relied upon for the safe design and operation of the end item.

The Commercial Provider shall be responsible for updating non-compliance risk assessment and coordinating agreement/concurrence through all the appropriate technical forum(s), prior to presentation to the safety review board. In addition, the Commercial Provider is responsible for presenting the Non-Compliance/Variance through all necessary Contractor and NASA program control board(s) <TBR 3-3>.

Phase III HR approval is contingent upon CLDP approval of the associated Non-Compliance/Variance.

3.3.1 SAFETY NON-COMPLIANCE/VARIANCE DOCUMENTATION

The Commercial Provider develops non-compliance/variance data, in which the documentation adheres to the following:

- a. Safety Requirement(s) not met:
 - Explanation of the safety requirements not met.

- This will call out specific sections of the safety document that the hazard control is non-compliant with.
- b. Description of Non-compliance:
 - A brief summary or description of the safety non-compliance.
 - Effectivity date, if applicable.
- c. Reason for Nonfulfillment:
 - Briefly summarizes the reason the safety requirement cannot be met.
 - Nominally the project is primarily responsible for identifying why they cannot comply with the identified safety requirement (ex: technical complexity, loss of science, cost or schedule impacts, etc.)
- d. Rationale for Board Acceptance:
 - NASA accepts the rationale/basis for risk acceptance of the safety non-compliance.
 - The standard closure documentation statement added by NASA.

The Commercial Provider will present NASA (within the HR Cause or preferred format) the reason their design cannot meet requirements, why they need a Non-compliance/Variance, and their proposed rationale as to why the NASA should accept this condition.

All members of the Safety Reviews have an important role by evaluating the risk and providing a discussion in the safety reviews. The Chairs acknowledge concerns raised by the board members and weighs those concerns when deciding acceptance of risk. If a board member feels their concerns are not appropriately considered, they can raise their dissenting opinion through the NASA program control board(s). Additionally, each of the Technical Authorities can raise dissenting opinions through the CLDP PCB.

3.3.2 EQUIVALENT SAFETY NON-COMPLIANCE/VARIANCE

An ES Non-Compliance/Variance is one where the level of risk accepted is low in the judgment of NASA. NASA will accept equivalent risk when hazard control strategies have limitations or uncertainties, or when complete verification evidence is not available. If the risk falls outside the responsible level of risk acceptance by the NASA safety review board, the noncompliance will be elevated to the NASA PCB. However, robust alternative rationale or flight rationale must be in place to justify accepting the elevated risk posture. In the case where flight equipment design provides comparable (equivalent) or a higher degree of safety than if strictly compliant with a specific design requirement, an ES Non-Compliance/Variance is submitted for program assessment and approval.

Equivalent Safety considerations/criteria are identified in Table 3.3.2-1:

TABLE 3.3.2-1 EQUIVALENT SAFETY CONSIDERATIONS/CRITERIA (2 PAGES)

ES #	Consideration	Criteria
ES-1	How reliable are the existing controls? What are the margins of safety for the existing controls?	Other Factors Affecting Failure Tolerance and Design for Minimum Risk Areas. The consideration of equivalent safety/accepted risk will only be used when it is determined that the hazard control or safety verification method being utilized meets the intent of the safety requirement without increase of safety risk. If the hazard control is required to meet failure tolerance criteria, the design must be at least single failure tolerant to prevent the hazardous consequences. If “design for minimum risk” criteria apply to the control of the hazard, then the “other factors” considerations must establish that the intent of the requirement being addressed in the Acceptance rationale has been met.
ES-2	What is the window of vulnerability to the hazardous condition? Have we assessed all phases where this hazard can occur? What is the TTE for the hazard?	1FT to a Catastrophic Hazard with a Limited Time of Exposure. Reduced time of exposure to hazard causes may be considered the equivalent of additional FT in some specific flight safety situations. This consideration applies to designs where it has been determined that preexisting failures will have been detected and all failures causing the hazard must occur within a very limited time window. ES is possible only if it can be established that the design will be 1FT during the limited time of exposure.
ES-3	What is the likelihood of the hazard or hazardous effect occurring?	1FT to a Catastrophic Event where the Probability of the Catastrophic Effects, after Two Failures, are 1×10^{-4} or less. If the probability of occurrence, after two failures, approached the probability of failure of an inhibit, the safety equivalent of a compliant design would be achieved. Consideration of this type of uncertainty will be included in the NASA deliberations, and when the probability of hazard occurrence after two failures reaches 1×10^{-4} or less, equivalent safety has been achieved.
ES-4	What is the flight history of this end item? What is the experience of the Commercial Provider relative to the situation involved?	Designs that do not satisfy 2FT and/or DFMR requirements, can be accepted when: a) The hazard is controlled through a defined process in which standards and margins are implemented. b) Environments are well understood. c) Production controls to ensure the produced hardware will have the expected performance. d) If the hazard control is required to meet FT criteria, the design must be at least 1FT to prevent hazard occurrence. e) If DFMR criteria apply to the control of the hazard, then positive margins must be demonstrated. f) Related deviations or waivers against approved design requirements or standards do not adversely affect the sufficiency of the hazard control. g) Verification methodology is robust (e.g. more heavily reliant on test vs analysis) and any verification related deviation or waivers do not adversely affect the sufficiency of the hazard control.
ES-5	What mitigations exist and is there time to execute them if the hazard occurs?	Designs that allow real time operational management of the hazard consequence with limited Time of Exposure. Operational controls to control reduced time of exposure to hazard causes may be considered the equivalent of additional FT if: a) The design is at least 1FT to prevent hazard occurrence. b) The system is controlled and monitored directly by the flight crew or mission control.

ES #	Consideration	Criteria
	Will the crew be notified if this condition occurs?	c) The window of hazard exposure is very limited and does not exceed the timeframe that is required for the flight crew or mission control to react to manage the hazard. d) There is sufficient time with reasonable margin to execute the hazard controls within the TTE.
ES-6	Is there any uncertainty in this situation?	1FT to a Hazardous Event where there is Significant Uncertainty as to whether or not the Event is Actually Catastrophic. It is extremely difficult to place some hazards in the proper hazard severity category (critical or catastrophic). In order to avoid unnecessary impacts to hardware due to an overly conservative safety policy, NASA will consider this uncertainty in its evaluation of HRs. The HRs will be assessed against the 2FT criteria necessary for the control of catastrophic hazards; however, if the design is at least 1FT to the hazardous event, and if in the engineering judgment of NASA, the hazard severity is sufficiently uncertain, equivalent safety will have been achieved and may be used as acceptance rationale.
ES-7	Human Factors.	Designs that Exceed Human Factors Safety Requirements. Human factors-type design criteria for sharp edges, pinch points, protrusions into translation paths, and touch temperatures are very conservative and provide adequate margin to protect the crew from hazards. However, due to the conservative nature of these requirements, there are many designs that have a noncompliance with these specific requirements, but still provide equivalent safety by alternate means/mitigations. These alternate means include caution or warning in crew procedures, protective devices, keep-out zones, hardware inspections and assessments by the flight crews, etc. With NASA approval of these alternate means, equivalent safety will be achieved.

The NASA Safety Review Board Chairs are authorized to accept risk via ES Non-Compliance/Variance in accordance with the criteria defined in Table 3.3.2-1. ES Non-Compliance/Variance will require the NASA Safety Review Board Chairs to inform the NASA Program Manager (PM) of the details of the ES Non-Compliance/Variance prior to approving HRs. Disagreements or exceptions to the ES criteria in Table 3.3.2-1 may be directed to the NASA PCB for resolution.

In some cases, where there are limitations or uncertainties in hazard control strategies or complete verification evidence is not available, the NASA Chair may accept elevated risk when there is a robust alternative rationale or flight rationale in place to justify accepting the elevated risk posture. ES non-compliance is when the level of risk accepted is low in the judgment of the NASA Chair.

3.3.3 PROGRAM LEVEL NON-COMPLIANCE/VARIANCE

Program level Non-compliances/Variations involve accepting significant risk and a rationale to accept the risk and approve the non-compliance/variance shall be presented by the Commercial Provider at the safety review board prior to presenting at the NASA PCB.

Additional NASA coordination/concurrence may be requested/required prior to receiving final NASA PM approval of safety program level Non-Compliances/Variations (ex: CLDP Safety and Mission Assurance Control Board). The Commercial Provider is responsible for documenting the Non-Compliance/Variance within the HR Cause and presenting the

Non-Compliance/Variance to the appropriate boards for review and concurrence prior to final approval.

If the Non-Compliance/Variance requires accepting significant risk, it is elevated to be a Program Non-Compliance/Variance requiring signature of the Destination PM.

The Commercial Provider is responsible for the words in the HR cause and for presenting the non-compliance to the appropriate boards for review/approval.

3.3.4 EFFECTIVITY OF NON-COMPLIANCES/VARIANCE

For those non-compliances/variances with limited effectivity, the Commercial Provider will correct the non-compliant condition prior to the expiration date or, as applicable, before any requested flight or operation of identical or similar items containing the previously documented safety deficiency.

4.0 SAFETY HAZARD ANALYSIS DEVELOPMENT AND SAFETY MILESTONES

The safety HA and review process are a phased safety review process (Phases 0, I, II, and III) that corresponds to the hardware's conceptual, preliminary, critical design and acceptance phases (including verification/validation).

The safety HA begins at the Concept Development phase with the assistance from all appropriate stakeholders and continues throughout the life of the end item (Destination, payloads, cargo and/or transportation systems). Every phased safety review requires an SDP.

The SDP shall include a System Safety Assessment Report (SSAR), or a tailored version, that encompasses the data requirements for the relevant phase safety review (for a summary refer to Section 4.1.1, SDP Documentation Strategies), HRs and any other supporting data (including but not limited to Section 4.1.3, Technical Data Supporting Hazard Analysis) necessary to justify and explain the contents of the HRs. The completion of the appropriate safety HA and the CLDP acceptance of the residual risk is a component of the success criteria for the Preliminary Design Review (PDR)/Phase I, Critical Design Review (CDR)/Phase II, and Design Certification Review (DCR) /Phase III milestones. Section 4.2, Safety Milestones, contains further details on SDP and HR data requirements.

The Commercial Provider shall align their HA development schedule to ensure that all hazard requirements, controls and verifications (design features, applicable standard, necessary testing, required inspections, etc.) are in place to support procurement, manufacturing, assembly, and testing. Failure to identify and implement the appropriate controls and verifications exposes the Commercial Provider to the risk of having to rework/redesign activities. At times, major updates to design or development approach may merit reassessment/delta reviews of prior safety milestones to ensure continued completeness of safety hazard documentation.

The Commercial Provider should coordinate the phased safety schedule with NASA to maximize effectiveness of both Commercial Provider and NASA participation. Appendix G, Best Practices for Safety Reviews Roles and Responsibilities, provides the recommended phased safety data submittal timeframe. The Commercial Provider should have Delta Phase Safety reviews if there are significant changes to the safety documentation due to a milestone review. Meetings outside of the formal phased safety reviews (i.e., Working Groups (WGs), Technical Interchange Meetings (TIMs)/special topics) are encouraged to enhance efficiency and reduce the time required for safety data to be reviewed during the milestone review.

For larger, more complex systems with extensive safety HA/HRs, phased safety reviews may be divided across multiple meetings. These meetings could commence well in advance of the milestone review to ensure the phased review is completed prior to the conclusion of the milestone review. A summary of the development schedule and phased safety review timing, expectations and review scope is shown in Table 4.2-1, Safety Milestones and Development Schedule.

4.1 SAFETY DOCUMENTATION

4.1.1 SDP DOCUMENTATION STRATEGIES

The result of HA is typically documented in the form of HRs, contained in an SDP, and includes hazard identification, classification, resolution, and a record of all failures and anomalies. Prior to conducting each phase safety review, the Commercial Provider is required to submit an SDP which reflects the current design phase and corresponds to the current safety review. The SDP encompasses all pertinent safety information related to the system design for that phase.

The SDP at a minimum includes the following:

- a) Hardware/design overview and description,
- b) Operational description,
- c) Planned maintenance,
- d) Interface description/diagrams,
- e) Drawings/schematics of all components,
- f) HRs and Safety Non-compliances/Variations, as applicable,
- g) CSM Documentation

It serves as formal documentation confirming the system has been evaluated for any potential safety risks and associated mitigation has been thoroughly considered and verified. As the design evolves, the SDP is updated to address any changes.

Appendix E, Best Practices for Safety Data Development, contains additional SDP documentation best practices.

4.1.2 HAZARD REPORTS

HRs document hazard control(s), verifications, crew survival methods and emergency response procedures identified in the HAs for critical and/or catastrophic hazards. The HRs inform program management of risks, how the risks are managed and controlled, whether the residual risk is acceptable, and whether actions need to be taken to address the residual risk prior to proceeding to the next program milestone. The evaluation/classification process is approached in terms of ratings of hazard characteristics and consequences.

Appendix E.1, Hazard Reports, contains additional HR development strategies.

The level of detail provided in the HRs will depend on the maturity of the safety phase at which they are written (refer to Table 4.1.2-1, Levels of Maturity).

A checklist outlining the supporting data needed for each Phase by the various engineering technical disciplines and CLDP to support the hazard control and verification sections of the HRs is provided in Table 4.1.3-1, Technical Data Supporting Hazard Analysis.

TABLE 4.1.2-1 LEVELS OF MATURITY

Product Maturity	Review Phase	Report Content
Conceptual Design/PDR	I	Hazard and hazard controls identified
CDR	II	Hazard controls documented and hazard control verification defined
DCR	III	Hazard control verification defined/complete, data delivered, reviewed and closed*
Configuration Control, Delivery	Post III	Safety verification tracking complete. All hazard control verifications closed.

*All verifications that are not complete/closed at the Phase III level review should be documented for safety verification tracking (See Section 4.2.7, Safety Verification Tracking).

4.1.2.1 HR STRUCTURE

Each hazard identified shall have its own HR and contain a description of the hazard and its effects and contains one or more causes that can lead to the hazardous condition. Each cause contains one or more controls for preventing the cause from occurring. Each control contains one or more verifications, confirming that the control is valid. All HRs shall include the data specified in Tables 4.1.2.1-1 through 4.1.2.1-4 at the minimum. The first table covers the overall hazard data, the tables that follow covers the data needed in the subsections of the HR.

TABLE 4.1.2.1-1 HAZARD REPORT DATA (3 PAGES)

HR Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
Hazard Report Number	A systemic unique reporting number	Created	-	-
Hazard Report Title	Brief description of the hazard in the form of an HR title	Initial title	Updated title	Final title
Date Created/ Revised	Provide the date the HR was entered or revised.	Latest revision date	Latest revision date	Latest revision date
Safety Review Level	Enter the phase safety review level maturity (Phase I, Phase II, or Phase III).	Enter "Phase I"	Enter "Phase II"	Enter "Phase III"
Hazard Severity	Designate if the hazard is Critical and/or Catastrophic.	Initial designation	Updated designation	Final designation
Hazardous Condition Description	Include a description that defines the risk situation including the unsafe act or conditions and its	Initial description	Updated description	Final description

CLDP-STD-3102
Baseline - DRAFT

HR Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
	effect on Commercial LEO Destination System or personnel, including: a) System/subsystem fails to operate as intended b) Inadvertent operation			
Interfaces	Identify the different interfaces (e.g., modules, components, and/or transportation systems). Include all hardware that will be part of the control strategy for the hazard.	Initial description	Updated description	Final description
Scope of the Hazard	Describe the scope of the hazards being addressed including, as appropriate, the end item, system, subsystem, operation and related hazards and their reports.	Initial scope	Updated scope	Final scope
Hazard Remark	Description of the hazard and its effects. Reference applicable NASA Standards, Requirements, JSC documents, and other relevant data. Include information related to the hazard that is not covered elsewhere.	Initial remarks	Updated remarks	Final remarks
System/Subsystem	The project system/subsystem associated with the hazard	Provide system/subsystem	Provide system/subsystem	Provide system/subsystem
Mission Phase	Describe applicable Mission Phases (e.g. Assembly/Reconfigure	Provide Mission Phase	Provide Mission Phase	Provide Mission Phase

HR Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
	ation, Dynamic ops, Launch, etc.)			
Flight/Mission	Provide assigned flight or mission	Provide flight or mission	Provide flight or mission	Provide flight or mission
Cause Summary/List	List the titles of causes associated with this hazard, include a severity and likelihood rating of the cause.	Provide Cause list	Provide Cause list	Provide Cause List
Action Items	List of open and closed action items and their titles and descriptions	Initial List	Updated list	Final List

TABLE 4.1.2.1-2 HAZARD REPORT DATA - CAUSES

HR - Causes Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
Hazard Cause Title	Brief description of the cause of the hazard in the form of a cause title	Initial title	Updated title	Final title
Hazard Cause Severity	Designate if the cause is Critical and/or Catastrophic.	Initial designation	Updated designation	Final designation
Hazard Cause Likelihood	The likelihood (probability of occurrence) of the hazard cause after controls have been implemented	Initial designation	Updated designation	Final designation
Hazardous Cause Description	Include a description of key factors that lead to the expected outcome/consequence.	Initial description	Updated description	Final description
Hazard Cause Remarks	Include any information relating to the hazard but not fully covered in any other item field,	Initial remarks	Updated remarks	Final remarks
Failure Tolerance/DF MR Approach	Identify if the cause is controlled by 1 or 2FT, DFMR, or defined at the individual control level.	Preliminary designation	Updated designation	Final designation
Crew Survival Methods	Describe, if applicable, the technique used to ensure crew survivability.	Initial CSMs	Updated CSMs	Final CSMs

Destination Survival Methods	Describe, if applicable, the technique used to ensure destination survivability.	Initial destination survival methods	Updated destination survival methods	Final destination survival methods
------------------------------	--	--------------------------------------	--------------------------------------	------------------------------------

TABLE 4.1.2.1-3 HAZARD REPORT DATA – CONTROLS (2 PAGES)

HR - Controls Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
Control Title	Brief description of the implemented control in the form of a control title	Initial title	Updated title	Final title
Control Type	Provide a designation of the control type. Identify if the control is a design control, process control, software control, Operational control, safety Non-Compliance/Variance (Equivalent Safety or Program Level), or if the control is a transfer to another cause or HR control. Note: The hazard controls should be numbered to provide linkages with the Methods of Verification of Controls	Initial designation	Updated designation	Final designation
Control Description	Include a description of the design/operational controls needed to mitigate the hazard cause, including existing technical requirements (e.g., factors of safety, design standards, etc.). Note: Sufficient detail will be provided to clearly reflect controls which mitigate/control the hazard. Note: For operational controls, provide an initial description of the real-time activities of the on-orbit crew, issuance of a ground command or the implementation of a	Initial control description	Updated control description	Final control description

HR - Controls Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
	preplanned decision by the Flight Control Team, or Crew Training.			
Failure Tolerance/DFMR Approach	If the failure tolerance/DFMR approach at the hazard cause level specified that the approach will be defined at the control level, define if the approach is One or Two failure tolerance or DFMR. Otherwise, enter, "Not Applicable"	Preliminary designation	Updated designation	Final designation

TABLE 4.1.2.1-4 HAZARD REPORT DATA – VERIFICATIONS (3 PAGES)

HR - Verifications Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
Verification Title	Brief description of the verification method in the form of a verification title.	-	Initial title	Final title
Verification Description	Clearly include sufficient detail or explanation of the testing, inspection, or analysis which mitigates the hazard to support hazard closure or risk acceptance.	-	Initial description	Final description
Verification Status	Indicate if the verification is open, closed, or closed under a safety verification tracking method.	-	Initial status	Final status Note: All verifications should be closed or closed under a safety verification tracking method.
Verification Timing	Identify if the verification closure documentation will be delivered at one of the following timing categories: A – "At Phase III Data Submittal"; B – "Before Signatures"; C – "Closed to safety verification tracking"	-	Proposed verification timing	Finalized verification timing

CLDP-STD-3102
Baseline - DRAFT

HR - Verifications Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
	Note: Analysis and test verifications are nominally an A timing. Demonstrations and other verifications requiring closure prior to SDP approval are nominally a B timing.			
Verification Occurrence	Identify how often the method needs to be verified: Verified once (including per unit or lot) or for every flight/Increment	-	Proposed occurrence	Final occurrence
Verification Closure Documentation	Indicate the documents/location in which the documents are stored for verification closure rationale	-	Initial closure documentation Note: Only applicable at Phase II if the verification method is already closed	Final closure documentation for all verifications Note: Identify the verifications closing under a safety verification tracking method
Verification Estimated Closure Date (ECD)	Indicate the verification ECD	-	Proposed ECD	Final ECD
Verification Types	Indicate if the verification type is one of the following: Analysis: Technical evaluation of design Testing: Operation of the end item at flight conditions/environment Inspection: A physical measurement or evaluation of the flight hardware Demonstration: Qualitative demonstration by operation under flight conditions Transfer: Verification applicable	-	Initial verification type	Final verification type

HR - Verifications Data	Description	Applicability (recommended)		
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)
	elsewhere. Reduces duplication of verification reports Operational Control: Verification is acceptance of the documentation into the operational control database and agreed operational control is in place or the inputs to the products are completed			

4.1.3 TECHNICAL DATA SUPPORTING HAZARD ANALYSIS

The SDP shall include the applicable supporting data content and maturity in accordance with Table 4.1.3-1, Technical Data Supporting Hazard Analysis. This content is required to support the hazard control and verifications sections of the HRs. The HA data should clearly identify the design baseline on which it is based.

TABLE 4.1.3-1: TECHNICAL DATA SUPPORTING HAZARD ANALYSIS (11 PAGES)

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
Structures (including pressurized, unpressurized, and composite hardware as applicable)	1. Preliminary Structural Verification Plan in accordance with JSC 65828	Draft Plan	Final Plan	-	<TBR 4-1>
	2. Structural analysis report which verifies positive margin	-	Analysis Outline	Final Report	
	3. Structural Test Plan/Results	-	Preliminary Test Plan	Final Test Plan and Results	
	4. Fracture Control Plan in accordance with NASA-STD-5019	Final Plan	-	-	
	5. Fracture Control Summary Report	-	Status Report*	Final Report	
	6. Non-Destructive Inspection/Evaluation (NDE) Plan in accordance with NASA-STD-6016	Final Plan	-	-	
	7. Non-Destructive Inspection/Evaluation Summary Report	-	Status Report	Final Report	
	8. Summary of design conditions for each pressurized system and how Maximum Design Pressure (MDP) was established	Initial Report**	Updated Report**	Final Report**	
	9. Leak Analysis report, identify maximum acceptable leak rate(s) and how leak rate(s) are established and verified in accordance with NASA-STD-7012	-	Status Report	Final Report	
	10. Qualification test plans/report (i.e., proof testing, non-destructive testing)	-	Test Plans	Final Test Reports	
	11. Acceptance test plans/report (i.e., proof testing, non-destructive testing)	-	Test Plans	Final Test Reports	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
Pyrotechnic Devices	1. Identification of pyrotechnic devices (pyrotechnic quantities) and functions performed	List w/Functions	Updated List	Final List	
	2. Pyrotechnics Verification Plan in accordance with JSC 62809	Draft Plan	Final Plan	Summary of Verification Results	
	3. Propellant Description Sheets	Draft Sheet	Final Sheet	-	
	4. Component Material Safety Data Sheet (MSDS)	Applicable MSDS	-	-	
	5. Acceptance and qualification plans and test reports	Draft Plan	Updated Plan and Initial Report	Final Report(s)	
Materials	1. Materials and Processes Selection, Control, and Implementation Plan in accordance with NASA-STD-6016	Final Plan	Revision (if applicable)	Revision (if applicable)	
	2. Materials and Processes verification	-	Status Report	Final Report	
	3. Materials Identification and Usage List (MIUL) per NASA-STD-6016	Initial List	Updated List	Final List	
	4. Materials Usage Agreement (MUA) per NASA-STD-6016	Initial Form	Updated Form	Final Form	
	5. Volatile Organic Compound Usage Agreement (VUA)	Initial Form	Updated Form	Final Form	
Fire Detection /Suppression	1. Fire Detection and Suppression (FDS) Implementation Approach	Initial Description	Updated Description	Final Description	
Ionizing Radiation	1. Review of design to verify all radioactive materials a documented	Initial List	Updated List	Final List	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	2. Review of design to verify flight and ground crew exposure is minimized in accordance with Federal licensing standards	Draft Form DF44	Updated Form	Approved Form	
	3. Review of design for containment provisions	-	Drawing Review	Final Inspection Report	
Non-Ionizing Radiation	1. List of equipment generating non-ionizing radiation	Initial List	Updated List	Final List	
	2. List identifying each laser, its operating location, complete beam path, hazard classification (per ANSI Z136.1) and operating characteristics	Preliminary List	Final List	Summary of verifications and Test Results	
	3. Tailoring/Interpretation Agreement	Initial Form	Updated Form	Final Form	
Ground Commanding	1. List of hazardous commands	Initial List	Final List and Draft Implementation Plan	Verification of Implementation	
	2. Hardware (HW)/ Software (SW) Controls	Initial List	Final List and Draft Implementation Plan	Verification of Implementation	
	3. Procedure input used to preclude inadvertent commanding	Initial List	Final List & Draft Implementation Plan	Verification of Implementation	
	4. Description of command system	Initial Description	Completed Description	-	
	5. Training plan for command controllers	Initial Plan	Final Plan	-	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
Robotic Operations	1. List of hazardous operations	Initial List	Final List & Draft Implementation Plan	Verification of Implementation	
	2. HW/SW Controls	Initial List	Final List & Draft Implementation Plan	Verification of Implementation	
	3. Procedure inputs used to preclude inadvertent operations	Initial List	Final List & Draft Implementation Plan	Verification of Implementation	
	4. Description of robotic operations system	Initial Description	Completed Description	-	
Electrical Systems	1. Wire sizing and circuit protection diagram	Initial Diagram	Updated Diagrams	As Built Diagrams	
	2. Workmanship testing (i.e., burn-in screening, thermal cycle, vibration)	-	Final Plans	Final Reports	
	3. Qualification testing (i.e., bonding, grounding)	-	Final Plans	Final Reports	
	4. Review of design to verify design features that preclude crew contact with powered components, wires, or connectors	-	Initial Review	Final Verification	
	5. Identification of devices that may have arcing/sparking potential. Review test data or vendor specification to verify hermetic seals.	Initial List	Summary of Vendor Data	Final Report	
	6. Review of test data or thermal analysis to verify the maximum temperature and the potential for ignition sources	-	Initial Analysis and Test Report	Final Report	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	7. Identification of potential sources for static electrical discharge. Review test for static discharge techniques and groundings inspections.	Initial List	Updated List	Test Data and Inspections	
	8. Review of design to verify design features that preclude mis-mating of connectors	-	Plan for Features	Verification of Implementation	
	9. Wire cable routing and connectors for redundancy separation	Initial Diagram	Updated Diagrams	As-Built Diagrams	
Components and elements of mechanisms in critical applications	1. Identification of critical procedures, processes, and inspection points	Initial List	Final List	-	
	2. Mechanisms verification plan in accordance with verification requirements of NASA-STD-5017	Draft Plan	Final Plan	Verification of Implementation	
Hazardous Materials (toxicological, biological, ECLSS, and flammable)	1. Hazardous Materials Summary Tables (HMSTs) or equivalent	Preliminary	V1 Updates	V2 – Final Verified	
	2. Off-gas testing in accordance with NASA-STD-6016	Final Plan	-	Materials and processes verification Final Report	
	3. Analysis to validate that all hazard controls, including margins of safety, materials compatibility, levels of containment and/or failure tolerance verifications are acceptable	-	Draft Report	Final Report	
Mechanisms	1. Inspection of drawings	-	-	Inspection Report	
	2. Design Life Testing	-	Test Plan	Test Report****	
	3. Thermal cycle tests	-	Test Plan	Test Report****	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	4. Thermal-vacuum tests	-	Test Plan	Test Report****	
	5. Vibration tests (environmental and acceptance)	-	Test Plan	Test Report****	
	6. Review of design to verify the minimization of sharp edges, and that remaining sharp edges are not exposed or are not on accessible structures.	-	Inspection Report	-	
	7. Sharp edge testing to verify that sharp edges are not exposed or accessible	-	-	Verification Report	
	8. Review of design to verify that pinch points are not exposed or accessible	-	Inspection Report	-	
	9. Procedure inputs that verify pinch point or sharp edge controls	-	Complete	Verification	
	10. Review of design to verify that hot/cold spots are not accessible	List of possible sites	Updated List & Initial drawing review	Final Inspection Report	
	11. Touch temperature testing	Test Plan	Updated Plan based on analysis	Final Test Report	
	12. Procedure inputs that verify touch temperature controls for exposed hot/cold surfaces	List of possible sites	Completed Procedures	Inspection Report	
	13. Structural verification	Preliminary Stress and Life Margins	Structural Analysis Reports (Stress and Life) and Static Test Plan	Updated Structural Analysis and Static Strength Test Report	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	14. Acoustic test results	Test Plan	Preliminary Testing Reports (if available)	Final Test Report****	
	15. List of mechanism status indications	Planned Indications	Update to Planned Indications	Final List of Indications	
	16. Performance (force/torque) margins	Calculated Margins	Update of Calculated Margins	Test-Verified Margin Values	
	17. Compliance with NASA-STD-5017	List of Deviations to Standard	Updated List of Deviations	Certificate of Compliance to Standard	
Battery operated systems	1. Identification of cell or battery chemistry and manufacturer, electrical configuration (voltage and capacity), environmental requirements, electrical safety schematics, limited life (shelf and service life) for battery certification memorandum.	Preliminary Design Safety Approval***	Draft Certificate and Schematics***	Final Certificate and Schematics***	
	2. Pre-flight, On-orbit and Post-flight Plan	Draft Plan	Final Plan	-	
	3. Qualification testing (lot testing where applicable)	-	Test Plan	Final Test Report	
	4. Acceptance testing	-	Test Plan	Final Test Report	
	5. Materials and toxicity certification memorandums	-	Draft Memorandums	Final Certificates	
Software	1. Software Requirements Specification	Preliminary	Updated	Final	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	2. Software Architecture/Design Description	Preliminary	Updated	Final	
	3. Software Test Plan and Procedure	Preliminary	Updated	Final	
	4. Software Test Report	-	Preliminary	Final – Closure of Defects	
	5. Software Change Reports	-	Preliminary	Updated	
	6. Software Configuration Management Plan	Preliminary	Final	Final (rechecked)	
	7. Requirements Mapping Matrix	Preliminary	Updated	Final	
	8. CBCS Compliance Matrix	Preliminary	Updated	Final	
	9. Software Assurance Classification	Final	Final version rechecked	Final version re-checked	
	10. Software Safety-Criticality Assessment	Preliminary	Updated	Final	
	11. Software Safety Plan	Final	-	-	
	12. Software inputs integrated into the System Safety Data Package (software HA, software faults and failure modes analysis)	Preliminary	Updated Draft	Final	
	13. Software Verification and Validation Plan (incorporation/implementation of software safety requirements into the Commercial Provider's design)	Preliminary	Final	Matrix complete and verified (test and verification complete with results)	
	14. Software Version Description Document (VDD)	-	-	Final - approved	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
Avionics	1. Avionics Schematics/Functional & Physical Diagrams	Preliminary Schematics and Design Diagrams	Updated Schematics (including safety critical subsystems, inhibits, controls, and monitors) and Design Diagrams	As-Built Schematics and Design Diagrams	
	2. Safety Critical Subsystem Lists	Preliminary Critical Subsystem Lists	Mature Critical Subsystem Lists	As-Built critical Subsystem Lists	
	3. Interface Descriptions (impacts on other subsystems)	Preliminary Interface Descriptions	Updated Interface Descriptions	Mature Interface Descriptions	
	4. Test Articles (including test description, results, and hazards addressed)	Preliminary Test Articles	Test Articles and Lessons Learned	Mature Test Articles	
	5. Verification Plan for Avionics	Preliminary Verification Approach	Detailed Verification Approach	Verification Test Results, Test Reports, Test Issues and Test Issues Corrective Actions, if applicable	
Communications	1. Nominal and off-nominal Communications Concept of Operations (CONOPS), for all mission phases.	Preliminary nominal and off-nominal CONOPS	Updated nominal and off-nominal CONOPS	Final nominal and off-nominal CONOPS	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	2. Communication system architecture diagrams, physical schematics, and functional schematics.	Preliminary diagrams and schematics	Updated diagrams and schematics	Final diagrams and schematics	
	3. Communication system requirements and interface documents	Preliminary documents	Updated documents	Final documents	
	4. Failure Mode, Effects, and Critical Analysis and list of single points of failure.	Preliminary analysis	Updated analysis	Final Analysis	
	5. Coverage and dynamic link budget analyses	Preliminary analyses	Updated analyses	Final analyses	
	6. Test-Like-You-Fly (TLYF) and simulation plans	Preliminary plans	Updated plans	Final plans	
Ground Support Equipment (GSE)	1. List of GSE (including to what flight hardware the GSE interfaces), corresponding requirements, and location of proposed use.	Preliminary list	Updated list (w/requirement verifications)	Final List (w/completed requirement verifications)	
	2. Ground operations flow chart	Preliminary flow chart	Updated flow chart	Final flow chart	
EMI/EMC	1. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) test plan (which includes how the hardware is divided for testing, how spares are handled, and any qualification vs acceptance test differences	Draft test plan	Final test plan	Test results/report	
Mechanical Fasteners	1. Fastener control plan (which tracks fastener purchases, counterfeit fastener countermeasures, where	Draft control plan	Updated control plan	Final control plan	

Category	Hazard Report Technical Supporting Data (or alternate)	Applicability (recommended)			NASA Reference Documents
		PDR (Phase I)	CDR (Phase II)	DCR (Phase III)	
	they are used, preloading calculation assumptions, positive locking pins, and basic quality control)				

* Status Report providing parts categorization and results of any analysis or Non-Destructive Evaluation.

** Preliminary pressurized system schematic and operating parameters (e.g., temperature, pressure, and other environmental conditions); Preliminary summary of the derivation of system MDP(s); Preliminary list of all system working fluids, their complete chemical composition, amounts, potential hazards (e.g., flammability, explosion, corrosion, toxicity) and hazard category (e.g., catastrophic, critical, non-hazard); Summary of pressure vessel(s) design and qualification approach

*** List of type and number of battery cells, cell size (capacity), cell chemistry, cell manufacturer, and model number.

**** Test reports should contain a record of all test failures and anomalies involving qualification of flight hardware.

4.2 SAFETY MILESTONES

For expectations and scope of each phased safety review, reference Table 4.2-1, Safety Milestones and Development Schedule, and Appendix F, Best Practices for Phased Safety Reviews, for data development guidelines and safety review success criteria.

DRAFT

TABLE 4.2-1 SAFETY MILESTONES AND DEVELOPMENT SCHEDULE (3 PAGES)

Phase	Timing	Expectations to Support Review	Scope of Review
0	SRR/SDR	Develop initial listing of hazard events applicable to hardware and software design and operations/PHA/PHL. Technical description of as-analyzed hardware/software design (highlighting safety- critical subsystems) and mission scenario. Conceptual drawings, block diagrams, conceptual procedures, and trade studies. Identify hazards, causes, and safety requirements and applicable specifications.	Present overview of design and operational concept. Evaluate Preliminary Hazard List unresolved comment dispositions. Communicate expectations for Phase I.
I	PDR	1. Develop SDP/SSAR (or a tailored version of it) to reflect the preliminary design: a) Identify hazards, b) Identify hazard causes, c) Identify and document risk (consequences, likelihood, and likelihood justification) for each hazard cause, d) Document controls for eliminating, reducing, or mitigating hazards, e) Identify integrated hazards, f) Document preliminary safety verification methods, if known, g) All failure and anomaly history, and h) Preliminary design drawings, functional diagrams, and descriptions, and interface control drawings. 2. Updated description of as analyzed hardware/software design (highlighting safety- critical subsystems) and mission scenario. 3. Preliminary CBCS compliance matrix to be reviewed by Computer Safety Panel. 4. Preliminary Maintenance Hazard Assessment (MHA)/Integrated Hazard Analysis (IHA). 5. Preliminary Software Common Cause/Mode Blackout Zone analysis 6. Determine compliance with CLDP-REQ-1130 safety requirements. 7. Identify Failure Tolerance Non-Compliance/Variance. 8. Determine Crew and Destination Survival Methods.	1. Present updated overview of design and operational concept. 2. Summarize hazard controls, preliminary safety verification methods (if known), and cause risk. 3. Evaluate Preliminary Hazard Analysis unresolved comment disposition. 4. Identify interface hazards and requirements inconsistencies. 5. Identify known safety non-compliances/variances. 6. Special topics/splinters. 7. Evaluate MHA/IHA. 8. Obtain NASA approval (via signed HRs or endorsement captured in meeting minutes). 9. Communicate expectations for Phase II.

CLDP-STD-3102
Baseline - DRAFT

Phase	Timing	Expectations to Support Review	Scope of Review
II	Critical Design Review (CDR)	- Refine and expand SSAR (or tailored version of it): - Updated hazard descriptions, causes, and controls, - Define hazard control verification methods i.e., analysis, test, inspection, demonstration, etc. - Document interfaces and mission operations procedures, plans, and timelines, and - All failure and anomaly history. - Technical description of to-be-built hardware/software design (highlighting safety- critical subsystems) and mission operations. - Updated CBCS compliance matrix to be reviewed by the Computer Safety Panel. - Updated MHA/IHA. - Determine compliance with CLDP-REQ-1130 safety requirements. - Determine Failure Tolerance Non-Compliance/Variance. - Determine Crew and Destination Survival Methods. - Final Software Common Cause/Mode Blackout Zone analysis	- Present updated overview of design and operational concept. - Summarize hazard controls, safety verifications, and Cause risk. - Identify known Safety Non-Compliance/Variance. - Identify interface hazards. - Evaluate Hazard Analysis unresolved comment dispositions. - Special topics/splinters (Failure Tolerance Exemptions, Crew and Destination Survival Methods, other). - Evaluate updated MHA/IHA. - Obtain NASA approval (via signed HRs or endorsement captured in meeting minutes). - Communicate expectations for Phase III.
III	Design Certification Review (DCR)	- Complete System Safety Assessment Report. - Finalize technical description as necessary to reflect the as-built hardware/software design and adjust mission scenarios. - Final CBCS compliance matrix to be reviewed by Computer Safety Panel. - Final MHA/IHA. - Hazard control verification references defined, safety data delivered, reviewed, and closed. - Identify open safety verification items (to be tracked under a method of safety tracking verification). - Approve ground processing. - Flight safety certificate or equivalent.	- Present final overview of design and operational concept. - Summarize hazard controls, safety verifications, and cause risk. - Summarize all open safety verification items via a method of safety verification tracking. - Resolve all Safety Non-Compliance/ Variance. - Evaluate final MHA/IHA. - Evaluate Hazard Analysis unresolved comment disposition. - Special topics (Failure Tolerance Non-Compliance/Variations, Crew, and Destination Survival Methods).

CLDP-STD-3102
Baseline - DRAFT

Phase	Timing	Expectations to Support Review	Scope of Review
			11. Final Safety Assessment approval/Obtain NASA approval (via signed SDP, Phase III HRs and flight safety certificate (or equivalent)).
Post Phase III	variance Weeks/ Verification Completion	1. Close open safety verification items. 2. Assess real-time changes. 11. For Flight – Submittal of Safety Certification for Flight Readiness to Destination Program Manager (PM).	12. Support CLDP Safety CoFR endorsement.

4.2.1 PHASE 0 – CONCEPT DEVELOPMENT

The Phase 0 Safety Review correlates to a SRR and/or SDR design milestone during the Concept Development phase. Phase 0 Safety Reviews provide an opportunity for interaction with the appropriate safety review board(s) early within the design phase and allows for initial feedback on safety hazards, preliminary causes, controls, and verification approaches, nominally documented within a PHA.

It is strongly recommended that the Commercial Provider conduct a Phase 0 Safety Review with NASA for complex items like space suits, modules, major subsystems, vehicles, or complex additions or modifications. For simpler items with limited complexity and vehicle integration, a streamlined approach may be utilized, such as combining Phase 0 and Phase I Safety Reviews.

When requirements are not met, the discussion should address how the design solution effectively controls hazards, the rationale for confidence in the proposed design solution/approach, and reasoning behind the associated risk is minimal and acceptable.

One of the ways to document the safety analysis at a Phase 0 maturity is with the PHA. The primary objective of the PHA is to identify all potential hazards (including integrated hazards), hazardous events, hazard causes, concept of operations, and to determine the Commercial Provider specific safety requirements for eliminating, reducing, or controlling the risk. This process encompasses the identification of the system's safety-critical functions and the derivation of software safety Commercial Provider specific requirements.

Results of the HA are used to ensure that proper safety Commercial Provider specific requirements are identified in the appropriate safety documents. The results of the PHA are documented in the Preliminary SSAR (or a tailored version of it) and included in the PHL.

4.2.2 PHASE I – PRELIMINARY DESIGN

The Phase I Safety Review will be conducted during the PDR timeframe. The primary objective of the Phase I safety review is to examine the SSAR or a tailored version, identify all potential hazards (including integrated hazards) and their causes, and assess the methods/hazard controls for eliminating, reducing, or controlling the risk, and applicable preliminary verification methods for these controls.

The PHA is updated during the Preliminary Design phase and the process for the PHA and required data elements for the HRs are included in both Section 4.1.2, Hazard Reports. The SDP, which includes an updated SSAR or a tailored version that encompasses the data requirements for the relevant phase safety review and HRs, is the document used to record this analysis. The SSAR or a tailored version of it contains pertinent information about the system under analysis, descriptions, and background data necessary to understand the system and analysis, references to milestone review data essential for understanding the analyzed system, the ground rules for the analysis, and hazards evaluated and excluded from further detail in HRs.

The Phase I Safety Review is the first required safety review in which the safety and crew and destination survivability of the system/end-item and associated operations are assessed and documented in a HR. This review will encompass a summary and status of issues, actions, and agreements that have emerged from the incremental reviews leading up to this milestone. Potential safety requirement non-compliances and initial assessment of maintenance hazards is also be identified. During the Preliminary Design Phase, the software safety Commercial Provider specific requirements are integrated into the software design, and the software design is evaluated for its effectiveness in mitigating hazard risk. All CSMs and destination survival methods for catastrophic hazards will be identified, including potential survival methods, a description of their role in ensuring crew survival under catastrophic conditions, and references to system Commercial Provider specific requirements (if applicable) will be provided. Any identified issues or anomalies that impact or potentially impact the hazard scope may result in an update to the HR.

4.2.3 PHASE II – FINAL DESIGN

The safety analysis and review process are continued during the final design phase. The Phase II Safety Review will be conducted during the CDR timeframe and will focus on examining the updated SDP (updated SSAR or a tailored version of it, and HRs). The primary objective of the Phase II Safety Review is to evaluate the updated analysis that reflects the detailed design and operations of the system/end item. This is to ensure that all hazards (including integrated and maintenance hazards) and hazard causes have been identified. For each cause, all hazard controls have been identified and implemented, and specific methods of verifying each control (e.g., qualification vibration test in accordance with XYZ test plan, flammability assessment, inspection of as built hardware, etc.) have been identified in verification plans and procedures. Additional Commercial Provider specific data requirements that need to be identified or updated include safety requirement non-compliances/variances.

During the Final Design Phase, the software design is evaluated to ensure that the software safety Commercial Provider specific requirements have been implemented as intended, the system is maintained in a safe state for all operational modes, and the implementation does not compromise any safety controls or introduce any new hazards. All CSMs and destination survival methods for catastrophic hazards will be identified and provided for review, including potential survival methods, a description of their role in ensuring crew survival under catastrophic conditions, references to system Commercial Provider specific requirements (if applicable), and verification information, such as documentation/analysis that supports the availability of the identified CSMs/destination survival methods. It is critical that detailed verification plans are provided, reviewed, and approved in Phase II to ensure that the hazards controls have adequate verification before the verifications are performed. If detailed plans are not available when Phase II is completed, supplemental reviews must be tracked and performed before Phase III begins. Any identified issues or anomalies that impact or potentially impact the hazard scope may result in an update to the HR.

4.2.4 PHASE III – FINAL ACCEPTANCE

The safety analysis and review process is completed during the final acceptance which encompasses fabrication, assembly, and test of the system/end item. The Phase III Safety Review will be conducted during the Design Certification Review (DCR) timeframe and will focus on examining the final updated SDP (final SSAR or a tailored version of it, and HRs). The primary objective of the safety review is to evaluate the effectiveness of the hazard controls, evaluate the results of the verification activity and ensure all hazard control verifications have been completed or have a closure plan and Estimated Completion Date (ECD), in support of the first Certification of Flight Readiness (CoFR) review.

The Phase III Safety Review will also focus on ensuring:

- a) All software safety Commercial Provider specific requirements, functions, controls and processes have been verified in unit, component, system and/or acceptance level tests
- b) All CSMs and/or destination survival methods are identified, their role in ensuring crew survival is provided, and reference to associated Commercial Provider specific requirements and verifications is included, and,
- c) Specific methods of verifying each control in flight fabrication, assembly and test process are identified in verification plans and procedures.

Results of all applicable failure analysis are also within scope of the Phase III Safety Review.

Safety reviews are completed prior to delivery of the hardware from the Commercial Provider to the ground support integrator.

4.2.5 FLIGHT SAFETY CERTIFICATE

A flight safety certificate or equivalent certifies that all necessary safety analyses have been performed in accordance with applicable safety requirements, and that associated verifications have been completed or transferred to a method of safety verification tracking. This tool allows for Commercial Providers to communicate the safety of end items transported, stowed and/or operated on transportation systems and Destination.

NASA and Commercial Provider Safety Review Board Chairs shall confirm that all safety assessments have been reviewed and approved by signature on a flight safety certificate or equivalent from the appropriate authorities.

Appendix F.1.6, Flight Safety Certificate Development, contains additional documentation guidelines.

4.2.6 VERIFICATION CLOSEOUT

Verification data (i.e. analysis, tests, demonstrations) shall be submitted to the safety review board(s) along with the Phase III safety data and documented in the appropriate HRs. Verification data development, distribution, review, and evaluation is an iterative

process to prepare for final certification. Access to data during development is essential to meet program milestones.

Commercial Providers are responsible for providing closed loop traceability from hazard controls to requirement verifications and supporting documentation (e.g., ops procedures, flight rules, flight software verification tests, as well as vehicle testing/Destination testing (re-flown vehicles or re-occupancy verifications)). It is important to establish a rigorous process that ensures clear traceability and verification through implementation to document how the controls are being implemented.

Modifications to controls and verifications and clear understanding of the impacts per the modifications shall be assessed, communicated in a timely manner to all stakeholders and incorporated into the respective HRs.

Appendix F.1.7, Verification Closeout, contains additional factors that typically drive schedule considerations.

4.2.7 SAFETY VERIFICATION TRACKING

Phase II will set expectations on which verifications should have data delivered either at the time Phase III data is submitted, after Phase III submittal, and/or track open verifications. Open verifications are identified as safety verifications that are not completed at the time Phase III HRs are approved. Those safety verifications are evaluated on a case-by-case basis for inclusion method of safety verification tracking.

Verifications, such as built to drawings, inspections, and operational controls can remain open during the review cycle. Verifications tracked are typically those that are closed at the launch site and considered low risk (no further review needed).

Verification items that remain open on the flight HRs and are determined to be a constraint to ground operations, shall be identified for both flight and ground. Appendix F.1.8, Best Practices for Safety Verification Tracking, contains additional documentation guidelines.

Rationale should be provided and submitted for closure to support ground processing safety.

Acceptance of open verifications is at the sole discretion of the safety review board Chair(s). Following approval of the Phase III HRs with open verifications, the Commercial Provider should submit the updated status of all open safety verifications in support of CLDP flight readiness milestone activities. Frequency of updated statuses is negotiated with the safety review board. A final status with approval of all included verifications, shall be provided to the safety review board(s) prior to ground or launch processing.

4.2.8 POST-PHASE III ACTIVITIES

It is the responsibility of the Commercial Provider to maintain up-to-date hazard analyses of all systems. Changes to design or operations (flight and ground systems) or anomalies (accidents or incidents involving flight, flight-like, and ground systems)

post-Phase III that may affect the safe design, operation of the system/end item or impact to USG crew and Utilization, shall be reviewed for safety impacts and may require a delta safety review, as determined by the appropriate safety review board defined in Section 5.0, Safety Review Roles and Responsibilities.

If an impact to a hazard control and/or verification is identified in any of these cases, the HR will need to be updated prior to reuse in its flight and/or ground configuration. New or revised HRs and supporting data may be necessary to reflect hazard acceptance rationale.

4.2.8.1 POST-PHASE III (PRIOR TO FLIGHT) SAFETY APPROVAL

Phase III approval by both NASA and Commercial Providers shall be required prior to launch, nominally at L-4 weeks. If the system does not have full safety approval at L-4 weeks, the remaining open verifications being tracked must have a specific technical reason to remain open and a closure plan that supports the current launch date. The Commercial Provider shall close all safety verifications required to show that the system/end item can be:

- a) Safely loaded on the launch vehicle and/or transportation vehicle, and,
- b) Safely stowed on the transportation vehicle and Destination.

Safety verification review effort for Commercial Providers becomes the critical path for certification of readiness.

Acceptable safety data to show a system/end item is safe for launch and stow include assurance of materials safety (i.e., flammability and offgassing), hazardous material containment/structural assessments, and stored energy/battery safety. Commercial Providers must also complete all safety verification testing/analysis/inspections that cannot be completed when the hardware is on a launch vehicle or on a Destination (i.e., electrical bonding/grounding test, pressure testing, inspection of hardware to design drawings, etc.). These verifications must be completed prior to the SRB Chairs' approval of system/end item for flight. An operational constraint will be placed on the system/end item to preclude on-orbit operations.

4.2.8.2 POST-FLIGHT SAFETY APPROVAL

For the system/end item that is safe for launch and stow with an operational constraint, Commercial Providers shall submit operations safety data to the appropriate SRB for full safety approval prior to on-orbit operations. Once the Phase III SDP/HRs addressing safe on-orbit operations are approved by the appropriate SRB Chairs, then the operational constraints can be removed.

4.2.8.3 ON-ORBIT RECONFIGURATION

An on-orbit reconfiguration is defined when:

- a) Systems will be physically reconfigured by modular addition/substitution and potential new hazards may arise from the new configuration, and/or,

- b) End items experience a change in intended use or manifest location beyond the approved safety HA.

Such modifications impact the requirements and baselined Phase III safety data. A delta safety assessment (updated SDP/HRs) shall be conducted prior to any on-orbit reconfiguration to identify new and invalidated hazards, hazard controls or verifications impacted by the change, including placing an operational constraint until verification is reassessed and closed, as needed. Controls and verifications to existing HRs are updated as applicable to the reconfiguration. Depending on the scope of the changes, the SRB will determine whether a delta Phase III safety review is sufficient, or if an entire phased safety review cycle is required.

4.2.8.4 MISSION UNIQUE HAZARDS

A new mission commences with the arrival of USG crew and ends with the departure of that crew. Mission operations and certification baseline should be addressed, reviewed, and approved with safety reviews approved in support of CoFR and be ready for flight readiness prior the mission/start of a new mission. Any mission unique hazard is identified as early as possible and must either be approved no later than L-4 weeks or follow the open verification tracking process in Section 4.2.7, Safety Verification Tracking. Mission analysis that is not complete at the start of the mission will be tracked as open work and completed prior to initiation of mission related activities. Critical operations will be assessed prior to execution. This is applicable to transportation systems (cargo and crewed vehicles), mission unique operations, and crew destination occupancy. Utilization missions will be analyzed prior to flight.

4.3 SERIES, REFLOWN, AND MODIFIED HARDWARE

The Commercial Provider is responsible for the safety of the series/reflow/modification items and associated interfaces by assessing the applicability of the previously approved safety data to the planned application. The Commercial Provider shall assess all series, reflow, and modified hardware each time they are manifested for transportation to ensure that the data supporting the original approval are still valid.

Appendix F.1.9, Series, Reflow and Modified Hardware, contains additional documentation guidelines.

5.0 SAFETY REVIEW ROLES AND RESPONSIBILITIES

The goal of the safety reviews is to assist the Commercial Provider in navigating through each of the safety review phases efficiently, during engagement with all applicable joint boards between the Commercial Provider and NASA. The safety reviews ensure the Commercial Provider's safety processes meet the intent of this document required for safe crew operations by:

- Assessing process maturity
 - Identify hazardous conditions
 - Understand the potential causes of the hazardous conditions
 - Consider relevant design changes
 - Built in appropriate FT or operational controls
 - Implement appropriate hazard controls

In order to meet the goal, the Commercial Provider and NASA will collaborate and establish a unified safety review process with shared approval authority, while providing a structured path for elevating unresolved issues.

The Commercial Provider shall develop, implement, deliver, maintain, and operate in compliance with a hazard analysis and system safety plan that grants NASA approval authority at safety reviews for hazard analyses that impact USG Crew and Utilization and meets the intent of CLDP-STD-3102.

The Commercial Provider shall perform safety reviews with NASA participation as a co-Chair and include the chartered members. Each Chair determines which and the number of subject matter experts from their team to attend. Meeting facilitation activities will be the responsibility of the Commercial Provider.

Engaging multiple safety boards may result in the inability to reach a consensus at the safety review (whether disagreement on the disposition of a HR, adequacy of a hazard mitigation or acceptability of residual risk). After a sufficient period of deliberation (as determined by the safety review board co-chairs), the issue will be elevated to the appropriate joint program control boards. Participation will be determined based on the type of safety review but, at a minimum, include the representatives from the programs involved in the disagreement.

See Appendix G, Table G.1-1, Mission Phase Safety Review Roles and Responsibilities, for various roles and responsibilities for the Commercial Provider and NASA across End-to-End (E2E) mission phases and all operational phases.

APPENDIX A - ACRONYMS AND ABBREVIATIONS

ACGIH	American Conference of Governmental Industrial Hygienists
AI	Action Item
ALARA	As Low As Reasonably Achievable
ANSI	American National Standards Institute
BSL	BioSafety Level
BOZ	Black Out Zone
CaTS	Cargo Transportation System
CaVV	Cargo Visiting Vehicle
CBCS	Computer-Based Control System
CCP	Commercial Crew Program
CDR	Critical Design Review
CIL	Critical Item List
CLD	Commercial LEO Destination
CLDP	Commercial LEO Development Program
CLDS	Commercial LEO Destination System
CMHA	Commercial Module Hazard Analysis
CoFR	Certification of Flight Readiness
CONOPS	Concept of Operations
COPV	Composite Overwrapped Pressure Vessel
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CPV	Constant Pressure Valve
CR	Change Request
CRS	Commercial Resupply Services
CSD	Commercial Spaceflight Development
CSM	Crew Survival Method
CSRB	Commercial LEO Development Program Safety Review Board
CTS	Crew Transportation System
CVV	Crew Visiting Vehicle
DCR	Design Certification Review
DFMR	Design for Minimum Risk
ECD	Estimated Completion Date
eLRODS	Electronic Launch, Return, On-Orbit Data Set
ECLSS	Environmental Control and Life Support System
EMC	Electromagnetic Compatibility

CLDP-STD-3102
Baseline - DRAFT

EMI	Electromagnetic Interference
ES	Equivalent Safety
EVA	Extra Vehicular Activity
FDS	Fire Detection and Suppression
FFBD	Functional Flow Block Diagram
FHL	Flammability Hazard Level
FIPS	Federal Information Processing Standards
FMEA	Failure Mode and Effects Analysis
FT	Failure Tolerance
GFE	Government Furnished Equipment
GNC	Guidance, Navigation and Control
GOTS	Government-Off-The-Shelf
GSE	Ground Support Equipment
GSRP	Ground Safety Review Panel
HA	Hazard Analysis
HEPA	High Efficiency Particulate Air
HMST	Hazardous Material Summary Table
HR	Hazard Report
HRL	Hazard Response Level
HW	Hardware
ICD	Interface Control Document
IHA	Integrated Hazard Analysis
IRB	Interface Requirements Baseline
IRD	Interface Requirements Document
ISS	International Space Station
ISSP	International Space Station Program
IV&V	Independent Verification & Validation
JPR	JSC Procedural Requirement
JSC	Johnson Space Center
KNPR	Kennedy NASA Procedural Requirements
KSC	Kennedy Space Center
L-	Launch Minus
LEO	Low-Earth Orbit
MDP	Maximum Design Pressure

CLDP-STD-3102
Baseline - DRAFT

MHA	Maintenance Hazard Assessment
MIUL	Materials Identification and Usage List
MNWF	Must Not Work Function
MOTS	Modified-Off-The-Shelf
MSDS	Material Safety Data Sheet
MSWG	Mechanical Systems Working Group
MWF	Must Work Function
N	No
N/A	Not Applicable
NASA	National Aeronautics and Space Administration
NASA-HDBK	National Aeronautics and Space Administration - Handbook
NASA-STD	National Aeronautics and Space Administration - Standard
NPR	NASA Program Requirement
O ₂	Oxygen
O&SHA	Operating and Support Hazard Analysis
OPR	Office of Primary Responsibility
OSB	Outside of Board
OSHA	Occupational Health and Safety Administration
PCB	Program Control Board
PDR	Preliminary Design Review
PEHA	Portable Equipment Hazard Analysis
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PLN	Plan
PM	Program Manager
PPE	Personal Protective Equipment
REQ	Requirement
RF	Radio Frequency
SDP	Safety Data Package
SDR	Systems Definition Review
SHA	System Hazard Analysis
SMA	Safety and Mission Assurance
SMAC	Spacecraft Maximum Allowable Concentrations

CLDP-STD-3102
Baseline - DRAFT

SME	Subject Matter Expert
SQA	Software Quality Assurance
SSAR	System Safety Analysis Report
SSHA	Subsystem Hazard Analysis
STD	Standard
SW	Software
SWHA	Software Hazard Analysis
TBD	To Be Determined
TBR	To Be Resolved
THL	Toxicity Hazard Levels
TLV	Threshold Limit Values
TIM	Technical Interchange Meeting
TTD	Time-to-Detect
TTE	Time-to-Effect
US	United States
USCV	United States Crew Vehicle
USG	United States Government
WFF	Wallops Flight Facility
WG	Working Group
Y	Yes

APPENDIX B - GLOSSARY

ACCREDITATION

The process by which objective evidence is provided to verify and validate that all project requirements and processes are in accordance with CLDP certification requirements.

ACTION ITEM (AI)

Items that affect the fundamental basis of the HR (i.e., missing causes or controls) and require formal review by the boards.

AGREEMENT

Items that are considered mostly editorial in nature or to provide clarification. Agreements are typically closed outside of a formal meeting.

ANOMALY

A state or condition which is not expected. It may be hazardous but it is the result of a transient hardware or coding error.

BIOHAZARDOUS MATERIAL

Biological materials or agents that can be a risk to the health of humans, plants, animals, or negatively impact the performance of the spacecraft and its systems.

BLACK OUT ZONE (BOZ)

A flight phase in which hazard controls and mitigations do not provide sufficient time to prevent a catastrophic event.

CARGO

A Pressurized or unpressurized item, including vehicle-related hardware, science payloads, logistics, containers, and other items to be transported via hard-mount or soft stow to or from the Commercial LEO Destination.

CATASTROPHIC HAZARD

Any condition that when uncontrolled results in a catastrophic event. This is an event resulting in loss of life or permanent disabling injury, or an event resulting in the loss of a crew return vehicle.

COMMON-CAUSE FAILURE

Failure of 2 or more systems due to a single specific event or cause.

COMMON MODE FAILURE

A type of common cause in which the components fail in the same way or in the same mode.

COMPLEX ELECTRONICS

Complex electronics encompasses programmable and designable complex integrated circuits. "Programmable" logic devices can be programmed by the user and range from simple chips to complex devices capable of being programmed on-the-fly.

COMPUTER-BASED CONTROL SYSTEM (CBCS)

A control system which utilizes computer hardware, software, complex electronics and/or firmware which accepts input information, and processes that information to provide outputs to perform a defined task.

CONTROL

Design or operational features that provide a verifiable method of preventing the hazardous event from occurring (e.g., a switch that interrupts the power to a hazardous function).

CONTROL PATH

The logical sequence of flow of a control or command message from the source to the implemented effector or function. A control path may cross the boundaries of two or more computers. Portions of multiple control paths may exist in a single computer.

CREW SURVIVAL METHODS (CSMs)

Capabilities incorporated into program architecture and operations to preserve the crew's life in the presence of catastrophic conditions. Examples include abort, escape, and safe haven.

CRITICAL HAZARD

A hazard with a potential for non-disabling personnel injury or severe occupational illness; loss of Destination, mission or the ability to support a crewed mission over the planned mission duration.

DESIGN FOR MINIMUM RISK (DFMR)

A process that allows safety-critical systems to meet the intent of failure tolerance through robust design or other controls, such as factors of safety, high reliability, and other design margin techniques, rather than through redundancy.

The process should identify the standards and margins implemented to account for the absence of failure tolerance. The DFMR approach should also address environments the system will experience and process controls (e.g., non-destructive evaluation, test, etc.) required to ensure the integrity of the system. Examples of DFMR are structures, pressure vessels, pressurized line, material compatibility, and material flammability.

EMERGENCY SYSTEM

Emergency systems and equipment, such as fire suppression systems, fire extinguishers, emergency breathing masks, launch/entry pressure suits, ballistic unguided entry capability, and ascent aborts, are not to be considered part of the failure tolerance capability. Emergency systems are there to mitigate the effects of a hazard, when the first line of defense, in the form of failure tolerance, cannot prevent the occurrence of the hazardous situation. Pad and ascent abort systems are encompassed within the definition of emergency systems.

END ITEM

A final combination of end/final products, component parts, and/or materials that is ready for its intended use (e.g., module, module with transfer stage, utilization, etc.).

End items include, but are not limited to modules, Visiting Vehicles/Transportation Systems, payloads, logistics, crew psychological support items, tools, spare instruments, and assemblies, including waste.

ERROR HANDLING

An implementation (system or computer failure) mechanism or design technique by which software faults are detected, isolated, and recovered to allow for correct runtime program execution.

ESCAPE

A defect or nonconformance detected in a product that was released for operational use. This usually indicates a process flaw allowing the defect or nonconformance to escape detection (the processes were insufficient to capture the defect or nonconformance prior to product release).

FAILURE TOLERANCE (FT)

The ability to sustain a certain number of failures and still retain capability. A component, subsystem, or system that cannot sustain at least one failure is not considered to be failure tolerant. The ability to sustain a certain number of failures and still retain a specific capability (e.g., capability to continue the mission).

FAILURES

The inability of a system, subsystem, component, or part to perform its required function within specified limits. The discrepancy between the service provided by a faulty system or component and that described by an agreed upon specification.

FAULTS

An undesired system state and/or the immediate cause of failure (e.g., maladjustment, misalignment, defect, or other). The definition of the term "fault" envelopes the word "failure," since faults include other undesired events, such as software anomalies and operational anomalies. Faults at a lower level could lead to failures at the higher subsystem or system level.

FIRMWARE

The combination of a hardware device and computer instructions and/or computer data that reside as read-only software on the hardware device.

FREE-FLYER

An independent, unattached hardware, module, or vehicle in LEO. The hardware (such as cubesats) that could be jettisoned or orbiting in LEO. Vehicles (such as one-manned vehicles) that are livable, and independent from the modules.

GROUND SUPPORT EQUIPMENT (GSE)

Any non-flight equipment, systems, or devices specifically designed and developed for a physical or direct functional interface with flight hardware. Includes equipment used to support receiving, storage, transportation, handling, assembly, inspection, test,

CLDP-STD-3102
Baseline - DRAFT

checkout, service, launch, emergency egress, and recovery of space vehicles and payloads. The following are not considered to be GSE:

- Tools designed for general use and not specifically for use on flight hardware.
- Ground Support Systems that interface with GSE Facilities.

HAZARD

A state or a set of conditions, internal or external to a system, that has the potential to cause harm.

HAZARDOUS COMMAND

A command that can create an unsafe or hazardous condition which potentially endangers the crew or station safety. It is a command whose execution can lead to an identified hazard or a command whose execution can lead to a reduction in the control of a hazard. Commands which disable a must work function or enable a must not work function are considered hazardous.

HAZARD ANALYSIS (HA)

Identification and evaluation of existing and potential hazards and the recommended mitigation for the hazard sources and risk found.

HAZARD REPORT (HR)

The output of a safety analysis for a specific hazard which documents the hazard title, description, causes, control, verification, and status.

HAZARDOUS MATERIALS

Any item, substance, or agent (such as shatterable/physical, chemical, biological (biomaterials), and/or radioactive), which has the potential to cause harm to the crew, the habitable environment, and/or equipment either by itself or through interaction with other materials and/or factors such as flammability and toxicity.

INHIBIT

A design feature that provides a physical interruption between an energy source and a function (e.g., a relay or transistor between a battery and a pyrotechnic initiator, a latch valve between a propellant tank and a thruster, etc.) Note: Software inhibits or interlocks are not counted in meeting safety requirements for multiple inhibits.

INTEGRATED HAZARD ANALYSIS (IHA)

Integrated assessments (payload and/or systems) are developed by identifying interfaces that exist between the modules, assessing those interfaces with hazard potential, and documented results in the integrated analysis/integrated HRs. Any new or undocumented interface hazards are documented on a new HR.

INTEGRATED OPERATIONS

Operations starting one orbit prior to a Visiting Vehicle entering the Approach Ellipsoid and lasting until that vehicle leaves the Approach Ellipsoid on a non-return trajectory.

INTERLOCK

A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available. This ensures that any conditions

CLDP-STD-3102
Baseline - DRAFT

prerequisite for a given function or event are met before the function or event can proceed. Also referred to as a software inhibit.

LIKELIHOOD

Probability of occurrence of a hazard cause manifesting itself after controls have been implemented.

LOSS OF CREW

Death of or permanently disabling injury to one or more crew members.

LOSS OF MISSION

Loss of or inability to complete significant/primary mission objective.

MARGINAL

Any condition which may cause damage to an end item (the loss of which then itself does not constitute a critical or catastrophic hazard) and/or an injury that does not require medical intervention from a second crew member nor consultation with a flight surgeon (including those injuries that might result in minor crew discomfort). Marginal hazards do not require submission of HRs.

MITIGATION

A hardware/software design feature or an operational procedure that helps reduce the probability of realizing the hazardous event consequence.

MODIFIED HARDWARE

Hardware that is of a similar design and operation of other previously flown end items, but with modifications. Changes are considered "minor" if they do not affect the existing hazard controls and/or verifications. End items with significant re-design, changes to baselined controls/verification approaches and/or new hazards may warrant reclassification of the hardware as a delta-Phase III and require additional CLDP coordination and discussion.

MODULE

Permanent and non-permanent crew accessible portion on the Destination. The Destination Providers are responsible for the oversight of Commercial Providers building and outfitting Commercial Destination Modules for assembly, reconfiguration, or disassembly.

MUST NOT WORK FUNCTION (MNWF)

A function which, if performed inadvertently or at an inopportune time, results in a critical or catastrophic hazard as identified in the hazard reports.

MUST WORK FUNCTION (MWF)

A function which, if not performed, results in a critical or catastrophic hazard as identified in the hazard reports.

NON-COMPLIANCE/VARIANCE

Any technical non-compliances/variances, to specific safety requirements.

NONCONFORMANCE

Any deviation, failure, issue, or requirement violation of a software product or process to meet defined design, specification, standard, or requirement.

OPERATIONAL CONTROL

The control of a hazard by the real-time activities of the on-orbit crew, issuance of a ground command or the implementation of a preplanned decision by the Flight Control Team (FCT).

OPERATOR ERROR

An inadvertent action by flight crew or ground operator that could eliminate, disable, or defeat an inhibit, redundant system, containment feature, or other design features that is provided to control a hazard.

OUTSIDE OF BOARD (OSB)

Informal meeting that are coordinated and scheduled by a safety board engineer. These meetings are conducted to finalize disposition of HRs, assigned actions, and safety assessments that either do not require an additional formal phase safety review (as determined by the Board Chair) or has been previously dispositioned with minor changes.

OVERRIDE

The forced bypassing of required safety features (e.g. prerequisite checks on the operator-commanded execution of a function). Execution of any command (whether designated as a “hazardous command” or not) as an override is considered to be a hazardous operation requiring strict procedural controls and operator safing.

PHYSICAL AGENTS

Materials or substances that, alone, are considered non-hazardous but become hazardous when released in large mass or concentrations due to how they act and respond in microgravity.

PREREQUISITE CHECK

The validation by the CBCS that coded states or conditions necessary for the execution of a command has been met.

REFLOWN

Hardware (using the same part number and serial number) that have previously flown on a transportation vehicle or CLD, are unmodified in design and in scope of operations, and are being manifested to fly again.

SAFE HAVEN

A functional association of capabilities and environments that is initiated and activated in the event of a potentially life-threatening anomaly and allows human survival until rescue, the event ends, or repair can be affected.

SAFE STATE

A defined and deterministically achievable state in which all hazardous effectors are safe and no hazards are present. It includes, but is not limited to, identification of safe configuration for the state of the hardware, software, operational phase, device capability, configuration, file allocation tables, and boot code in memory. Note: The scope of safing necessary will be determined by hazard analysis.

SAFETY

A general term denoting an acceptable level of risk, relative freedom from and low probability of personal injury; fatality; loss or damage to vehicles, equipment or facilities; or loss or excessive degradation of the function of critical equipment.

SAFETY ANALYSIS

A systematic and orderly process for the acquisition and evaluation of specific information pertaining to the safety of a system.

SAFETY-CRITICAL

A condition, event, operation, process, function, equipment, feature, or system (including software and firmware) with potential to create a critical or catastrophic hazard. A safety critical feature of a design is a feature whose failure or malfunction has the potential to create a critical or catastrophic hazard. This terminology is most often used with structures, circuits, fasteners, software, and mechanisms. An end item with a safety critical feature does not classify the entire end item as safety critical. Safety critical may also be applicable to must-work and must-not-work designs when hazard potential is present.

SAFETY CRITICAL COMMAND

A command whose execution is necessary to prevent a hazardous condition or event.

SAFETY-CRITICAL SOFTWARE

Software is safety-critical if it meets at least one of the criteria in NASA-STD-8739.8:

- A. Causes or contributes to a system hazardous condition/event,
- B. Provides control or mitigation for a system hazardous condition/event,
- C. Controls safety-critical functions,
- D. Mitigates damage if a hazardous condition/event occurs, and
- E. Detects, reports, and takes corrective action if the system reaches a potentially hazardous state.

SAFE DESIGN LIFE

Time period in which an end item can be retained at or restored to the specified safe operational condition via prescribed resources and procedures. Safe design life is considered the end of useful life without extensive effort and/or expense and must include both ground and on-orbit time.

SAFE OPERATIONAL LIFE

Time period in which an end item will perform its intended function within specified performance limits under stated conditions without any corrective maintenance, recalibration or repair. Safe operational life must include both ground and on-orbit time.

SAFING

The sequence of events necessary to place systems or portions thereof in predetermined safe conditions.

SERIES

Hardware of the same design and operation as previously flown hardware, are built to the same drawings, have the same part number but different serial number, and use the same processes as the initial end item.

SEVERITY

The worst-case consequence of a failure, fault, accident, and/or undesired event resulting from this cause without taking into consideration controls or mitigations. Severity levels are Catastrophic, Critical, and Marginal.

SHATTERABLE MATERIALS

Any material that can fracture under a load or impact and produce fragments that are potentially hazardous to the crew and/or vehicle.

SOFTWARE (SW)

Computer programs and computer databases. As used in a CBCS, “software” refers to all flight software regardless of the media on which the software resides, including software that resides on hardware devices (i.e. firmware). This includes computer programs, procedures, scripts, rules, and associated documentation and data pertaining to the development and operation of a computer system. This also includes COTS, GOTS, MOTs, reuse, heritage, legacy, reused software, auto generated code, embedded software, firmware, and open-source software components.

SOFTWARE COMMON MODE FAILURE

A type of common mode failure in which every instance of the same software image executing on multiple devices encounters the same unexpected condition simultaneously or in a cascading sequence, adversely affecting the proper operation of the software and precluding the ability of redundancy management from isolating the problem to a specific device.

SOFTWARE ERROR

The difference between a computed, observed, or measured value, or condition, and the true, specified or theoretically, correct value or condition.

SOFTWARE FAULT

An incorrect step, process, or data definition in a computer system.

SOFTWARE INHIBIT

A software or firmware feature that prevents a specific software event from occurring or a specific software function from being available. This ensures that any conditions prerequisite for a given function or event are met before the function or event can proceed. Also referred to as an interlock.

SUBSYSTEM

Physical entities within a system that have functional capabilities allocated to them necessary to satisfy mission objectives. Subsystems can perform all allocated functions within a mission phase, or through mated operations with other Destination modules or subsystems.

SYSTEM

The collection of all space-based and ground-based systems (encompassing hardware and software) used to conduct space missions or support activity in space, including, but not limited to, the crewed space system, space-based communication and navigation systems, launch systems, and mission/launch control.

SYSTEM FAILURE TOLERANCE

A system design that fully controls a hazard should a software common cause/mode failure occur. This provides a fully functional redundant set of capabilities to avoid a catastrophic hazard (which may include dissimilar software or hardware, crew bypass capability, manual flight control, independent critical vehicle functions). Providing a fully functional redundant set of capabilities to avoid a catastrophic hazard is viewed as equivalent risk and meets the intent of failure tolerance requirements.

UTILIZATION

Inclusive term for science, research, technology development, industrialization, education, or outreach, regardless of the NASA (or OGA) sponsor.

VERIFICATION

The activity that establishes acceptable confidence of compliance with specifications. Verifications show proof of compliance with a requirement, or specifications based on a combination of test, analysis, demonstration, and/or inspection.

NOTE: When this term is utilized in conjunction with a HR, the set of verifications associated with a particular hazard control will provide necessary and sufficient evidence to validate that control.

WORKING GROUP (WG)

Informal meetings that may be held before or after a phase safety review to discuss detailed technical concerns and/or coordinate on resolution of issues in support of the safety review process.

APPENDIX C - OPEN WORK

C-1

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 2-1> is the first unresolved item assigned in Section 2 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	Status
TBD 2-1	2.1	Pending baseline approval of CLDP-STD-1150.	

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	Status
TBR 3-1	3.1.5	Additional Emergency Response and Crew Survival Method clarification.	
TBR 3-2	3.1.8	Finalize required fields for HMST documentation.	
TBR 3-3	3.3	Additional clarification to all NASA roles/responsibilities in the Non-Compliance/Variance process.	
TBR 4-1	4.1.3, Table 4.1.3-1	List of process documents as reference to each technical deliverable in Table 4.1.3-1, Technical Data Supporting Hazard Analysis. In addition, adjust the wording in the Ionizing Radiation and Non-Ionizing Radiation rows.	
TBR D-1	4.1.2, Appendix D	Common/standard list and HR template location/HR database	
TBR H-1	Appendix H	Additional clarification to all NASA roles/responsibilities for GFS Transportation	
TBR K-1	Appendix K	Additional clarification to all NASA roles/responsibilities for the Ground Safety process	

C-1

D-1 **APPENDIX D - BEST PRACTICES FOR HAZARD ANALYSIS TYPES**
 D.1 **HAZARD ANALYSIS**

Hazard analyses are performed by identifying, evaluating, and classifying a hazard.

In providing a method to analyze hazards, the resulting hazard analysis accomplishes the following:

1. Identifies hazardous conditions and hazardous elements in end item designs,
2. Addresses must work and must not work functions, including hazards from hardware and operational faults and failures,
3. Assesses the significance of the identified hazardous condition's effects,
4. Provides a basis for establishing system safety preventive measures,
5. Provides verification of end item design compliance to specified safety requirements and controls,
6. Examines the safety impact of failures,
7. Examines the hazard interface (through an integrated hazard analysis),
8. Assesses crew survival methods in the event available hazard controls have failed resulting in a catastrophic condition, and
9. Provides a basis to develop emergency response procedures.

The following list of hazard analyses are examples and not meant to be all inclusive: PHA, SHA, SSHA, PEHA, CMHA, O&SHA, SWHA, and Commercial Provider IHA. In conjunction with each of the above analyses, the applicable software should be evaluated for hazard potential. These primary analyses are described in Section D.2, Hazard Analysis Types.

D.1.1 **HAZARD IDENTIFICATION**

A hazard is the presence of a potential risk situation caused by an unsafe act or condition. Hazard identification is a process for determining and characterizing information relating to a hazard and documenting in a manner for management to review and understand.

To begin the hazard identification process, the Commercial Provider must become familiar with the design of the item to be analyzed as well as the environment and planned operations to be reviewed. Analytical effort and rationale should be documented progressively and systematically.

D.2 **HAZARD ANALYSIS TYPES**

Table D.2-1 describes examples of various HA techniques that can be utilized so that all hazards are identified. Utilizing all appropriate techniques at the stages identified helps ensure all hazards are identified.

D-2

TABLE D.2-1 HAZARD ANALYSIS TYPES

TYPE	PURPOSE	STAGE
Preliminary Hazard Analysis (PHA)	- Identify preliminary hazards (i.e., assembly complete and incremental assembly) and determine significance, - Establish safety requirements and critical limits, - Identify basic hazard controls, evaluate alternate concepts, and document initial safety risk of the concept or system, - Determine possible hardware, procedural, or system interface problems, and - Identify areas for testing, trade studies and further analysis.	System Requirements Review (SRR)/Conceptual Phase to eliminate possibility of costly design changes later.
Subsystem Hazard Analysis (SSHA)	- Identify hazardous conditions and elements in system/subsystem design and determine significance, - Establish a basis for hazard controls, and - Provide verification of system/subsystem design compliance to CLDP-REQ-1130 safety requirements and examines integrated hazards.	Preliminary Design Review (PDR)/Detailed Design Development as hardware drawings become available.
System Hazard Analysis (SHA)	- Examine safety impact of failures, - Examine hazard interface, and - Identify areas and provide specific detailed design information for additional analyses.	PDR/Detailed Design Development as system and subsystem design and interfaces (including software) are defined. SHA is updated because of any system and/or interface changes.
Portable Equipment Hazard Analysis (PEHA)	- Identify hazardous conditions and applicable Destination modules for a portable equipment item, - Establish a basis for establishing hazard controls, - Provides verification of portable equipment design compliance to specified safety requirements, - Examines safety impact of failure, and - Identify areas and provide specific detailed design information for additional analysis.	PDR/Detailed Design Development as hardware drawings become available.
Commercial Module Hazard Analysis (CMHA)	Identify hazardous conditions in Destination modules, and	PDR/Detailed Design Development as system and subsystem design and

D-2

D-3

TYPE	PURPOSE	STAGE
	Perform risk assessment on interfaces between the subsystems that compose the module.	interfaces (including software) are defined.
Operating and Support Hazard Analysis (O&SHA)	- Ensure the safety of system elements (personnel, equipment, software, and hardware) during and from operations, - Examine procedurally controlled activities, - Identify hazards associated with operations, including support operations (assembly, maintenance, resupply, refurbishment), - Identify hazard causes associated with mishap development associated with operations and support tasks, - Identify preventative procedures that can be used to avoid hazardous circumstances or mishaps, - Define requirements and timeline for emergency response and to support crew survivability assessments, and - Define requirements for handling and storage of hazardous materials.	SRR/PDR: An optimal approach involves two phases: perform a generalized analysis during the conceptual phase; and subsequently perform a specific and detailed analysis during the procedure development phase.
Software Hazard Analysis (SWHA)	- Software is evaluated as a cause of hazards, as an active control to hazards, and as part of the detection and warning system, - Integrated part of the system safety analysis for CLD, CTS, and CaTS safety reviews - Evaluate program and interface requirements, and identify errors and deficiencies in the program requirements that could result in a hazard, and - Requirements analysis defined by NASA-HDBK-2203.	Preliminary input to the system safety analysis.
Destination Provider Integrated Hazard Analysis (IHA)	- Identify interfaces between Destination modules/core systems/subsystems, - Identify interfaces between Destination, transportation systems, - Identify hazardous conditions to personnel and the system from the interactions with Destination modules/core systems/subsystems provided by other Commercial Providers/owners (integrated hazards), and	As early in the development process as possible.

D-3

D-4

TYPE	PURPOSE	STAGE
	Identify crew survival methods and emergency response processes.	
Maintenance Hazard Analysis (MHA)	- Identify all facets of maintenance activity that might result in a hazard, - Establish elements in the removal and replacement of hardware, including access paths for contact hazards, modification of existing safety features, and reverification of safety-critical features, and - State which hazard controls from baseline HRs are applicable, as well as perform an analysis to determine if any new hazards are present when performing the maintenance	As early in the development process as possible.
Ground and Mission Systems Hazard Analysis	- Ensure the safety of USG crew and NASA support personnel and integrity of the flight hardware prior to launch and after landing. <i>(Out of scope for CLDP-STD-3102)</i>	SRR/PDR

D.2.1 HAZARD ANALYSIS TYPES DESCRIPTION

D.2.1.1 PRELIMINARY HAZARD ANALYSIS (PHA)

The PHA is the initial effort in hazard analysis during the early design phases (Phase 0/TIM) that identifies top-level hazards and controls, provides a first look at the system risk, and provides the foundation for future analyses. The PHA provides the CLDP with knowledge of the potential hazard causes and candidate controls. The PHA should be used as the baseline for performing future analyses, such as the SSHA, SHA, and O&SHA. The PHA may be continued and updated during later phases.

The PHA is based on the best available data of the system or systems and how it will be used. Sources for data may include but are not limited to:

- System description documents,
- System diagrams,
- Mission descriptions,
- Operational concepts,
- Functional analysis/architecture documents,
- Functional Flow Block Diagrams,
- Mishap data from similar systems, and
- Lessons learned from other programs.

D-4

D-5 The PHA identifies and evaluates the hazards and hazardous events associated with the proposed design, operations and/or functions for potential hazard severity, time of exposure, and hazard classification. Design controls, software controls, operational controls and other actions needed to eliminate hazards or reduce the risk to an acceptable level should be considered and documented.

The PHA demonstrates a comprehensive analysis technique beginning with a top-level undesired event and continuing down to the identification of hazardous conditions or events and their corresponding causes that may be eliminated or controlled. When system redundancy is used as a control, common cause events should be considered.

The following steps are provided to assist the Commercial Provider and ensure the performance of a comprehensive PHA:

- Identify the hazardous conditions. Use the list of common/standard hazards in Hazard Database **<TBR D-1 >** as a guide. There may also be peculiar hazards associated with the subsystem being analyzed that are not listed. These should be added as “unique” hazards and appropriate hazard identification can be assigned as appropriate.
- Utilization of a comprehensive process to identify all the potential causes of the potential hazard. The causes will usually be from:
 - Hardware failure modes,
 - Personnel actions or inaction,
 - Anomalous or unexpected software behavior,
 - Component interactions,
 - Environmental condition(s) (induced or natural),
 - Energy sources, and
 - Operating conditions.
- Consideration of the following for identification and evaluation of hazards:

- D-6
- Hazard sources inherent to the design (e.g., propellants, lasers, explosives, toxic substances, corrosives, hazardous construction materials, pressure systems, and other energy sources). When assessing batteries, refer to JSC 20793, Crewed Space Vehicle Battery Safety Requirements, for information on identifying hazard, controls, and verifications. When assessing Lasers, refer to ANSI Z136.1, American National Standard for Safe Use of Lasers. Also, guidelines for conducting an oxygen compatibility analysis, including material system evaluations and test methods are identified in NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft.
 - Hazardous event occurrences producing the undesired consequences which include system failures, component failures, unexpected software behavior, or other events necessary for the consequences to occur.
 - Operating, test, and maintenance procedures (e.g., human error analyses of operator functions, tasks, and requirements; ergonomics; effects of factors such as equipment layout and lighting requirements; effects of noise or radiation on human performance; life support requirements and their safety implications in human systems; crash safety; egress; rescue; and salvage).
 - Facilities, support equipment (e.g., provisions for storage, disposal, assembly, checkout, proof-testing of hazardous systems and assemblies which may include toxic, flammable, explosive, corrosive or cryogenic fluids; radiation or noise emitters; and electrical power source), and training (e.g., training and certification pertaining to safety operations and maintenance).
 - Safety-related equipment, safeguards, and possible alternative approaches (e.g., monitoring, interlocks, system redundancy, hardware or software fail-operational/fail-safe design considerations, subsystem protection, FDS systems, Personal Protective Equipment (PPE), ventilation, and noise or radiation attenuation).
 - A review of historical safety experience (i.e., lessons learned on similar systems), including operator feedback.

Other aids, such as Sneak Circuit Analyses, FMEA/Critical Items List (CIL), and safety checklists, may be used to identify hazardous conditions and causes.

Analytical tools used by the Commercial Provider to perform comprehensive hazard analysis (such as fault trees, fishbone diagrams, etc.) should be provided at each phased review. The existing or proposed system safety, including software safety, requirement that will eliminate or control the hazardous condition should be identified.

A way to document the PHA would be using Table D.2.1.1-1, PHL Worksheet Sample Instructions, below. The hazard effect, severity level, system safety requirements (including software safety requirements) hazard elimination and control provisions columns should be completed when using this documentation method.

D-7

TABLE D.2.1.1-1 PHL WORKSHEET SAMPLE INSTRUCTIONS

Hazard Analysis Title:			Revision:		DRM:			
Worksheet No.:						Engineer:		
FFBD Version:			FFBD Block No.:			Date:		
Module/Subsystem:						Sheet:		

Hazard	Causes	Severity	Likelihood	Requirements	Hazard Elimination/ Control Provisions	Failure Tolerance	Emergency Response	Recommendation
Identify existing or potential hazards: Can the system fail to operate as intended? Can the system operate inadvertently (untimely)? Are there standard/common hazards? (See Appendix X.X).	Enter brief description of how each hazard is created (i.e., rupture of the O2 tank; wiring insulation overheating and igniting; human error, etc.) and identify the affected module (i.e., either initiates or is affected by the event). Record the potential effect of each hazard on critical equipment, personnel, the general public (i.e., emergency landing in inhabited area, etc.), and loss of mission/crew.	Identify the worst-case severity level as one of the following for each hazard as Catastrophic, Critical, Marginal	Provide the probability of occurrence of the hazard cause after controls have been implemented.	Identify the existing or proposed requirement that will eliminate or control the hazard by document and paragraph number.	Identify proposed hazard reduction methods for hazards.	Identify the level of failure tolerance required. How many levels of failure tolerance are currently in place? Does it meet the requirement?	Provide methods for crew and destination survivability.	Provide recommendations for additional requirements, trade studies, or other options which may be needed to control or eliminate the hazardous condition.

D-7

D-8 **D.2.1.2 SUBSYSTEM HAZARD ANALYSIS**

The SSHA is a safety risk assessment of a system's subsystems at a greater level of detail than provided in the PHA. The SSHA should occur when the preliminary design and concept definition are established and should continue through the detailed design of components, equipment, and software (Phase I level). The SSHA is updated as the result of any subsystem design change, new or modified hardware, and analyses of appropriate hardware and software failure history documented during the ongoing activity.

The SSHA verifies subsystem compliance with system/safety requirements, identifies previously unidentified hazards associated with the subsystem, assesses the risk of the subsystem design, considers human factors, functional and component failures, and functional relationships between components in the subsystem, including software, and recommends actions to control the hazards.

The hazards may be caused by loss of function, accidental activation, energy source, hardware failures, personnel actions or inactions derived from the system/module/Project O&SHA, failure of the software to behave as intended, interaction of components within the subsystem, inherent design characteristics, such as sharp edges, incompatible materials, and environmental conditions, such as radiation.

The SSHA defines the safety-critical functions, operations, possible component fault conditions, standard hazards, and safety-critical operations and environments associated with the subsystem.

The following steps are provided as a guide to assist the safety analyst and ensure the performance of a comprehensive SSHA:

1. Identify the hazardous conditions. Use the list of standard hazards in hazard database **<TBR D-1>** and software contributions as guides. There may be peculiar hazardous conditions associated with the subsystem being analyzed that are not listed in the figure. When assessing batteries, refer to JSC 20793 for information on identifying hazards, controls, and verifications.
2. All the potential causes of the hypothetical hazardous condition or event should be identified. The causes will usually be from:
 - a. Hardware failure modes,
 - b. Personnel actions or inaction,
 - c. Software failure modes,
 - d. Component interactions,
 - e. Environmental condition(s) (induced or natural),
 - f. Energy sources, and
 - g. Operating conditions.

D-9 D.2.1.3 SYSTEM HAZARD ANALYSIS

The purpose of the SHA is identical to the SSHA, but at the system (higher) level. Once the subsystem levels have been established, a combination of subsystems make up a system. In turn, a group of systems may compose another system until the top system is identified. Consequently, a system to one project may be a subsystem to another project. In general, the previous analyses are extended to encompass the total system. The unique aspect of the SHA is its view of interfaces between subsystems which make up a system. Hence, it is a form of an integrated HA.

The SHA effort will begin as a system and subsystem design, and interfaces, including software, are defined. The SHA will be updated when needed for system design, or interface changes, failure reports, and flight anomaly reports.

D.2.1.4 PORTABLE EQUIPMENT HAZARD ANALYSIS

The general purpose of the PEHA is to perform a safety risk assessment of a portable equipment item at a greater level of detail than that provided in a PHA and is very similar to the SSHA. The PEHA effort should begin when the preliminary design (Phase I level) and concept definition are established, and it should continue through the detailed design of components, equipment, and software. The PEHA should be updated as the result of any equipment design change, new or modified hardware, and analyses documented during the ongoing project activity of appropriate hardware and software failures history.

The PEHA verifies equipment compliance with system/safety requirements, identifies previously unidentified hazards associated with the equipment, assesses the risk of the equipment's design, considers human factors, functional and component failures, and functional relationships between components in the equipment, including software, and recommends actions to control the hazards.

The hazards may be caused by loss of function; accidental activation; energy source; hardware failures; personnel actions or inactions derived from the systems/module O&SHA; software deficiencies derived from the SWHA, interaction of components within the equipment, inherent design characteristics, such as sharp edges, incompatible materials; and environmental conditions, such as radiation.

The PEHA defines the safety-critical functions, operations, possible component fault conditions, standard hazards, and safety-critical operations and environments associated with the equipment.

D-10 D.2.1.5 COMMERCIAL MODULE HAZARD ANALYSIS

The general purpose of the CMHA is to perform a detailed safety risk assessment of a Commercial Module within the system and the interfaces between the subsystems that compose the module. The CMHA is identical to the SSHA, but at the module level. In general, the previous analyses are extended to encompass the total module. The unique aspect of the CMHA is its view of interfaces between subsystems which make up a module.

The CMHA verifies module compliance with safety requirements and identifies previously unidentified hazards associated with the subsystem interfaces, module functional faults and module operation in the specified environment. The CMHA considers human factors, element/functional failures and functional relationships between subsystems comprising the module, including software. The CMHA identifies existing controls and recommends additional controls.

The CMHA effort should begin as module and subsystem designs, and interfaces, including software designs, are defined. The CMHA should be defined for the Phase I safety level. The CMHA should be updated when needed for module design or interface changes, failure reports, and anomaly reports.

Test information, such as failure history or other anomalous conditions encountered during test and development should be a major consideration when judging the effectiveness of hazard controls and assessing risk. Failure history is the record of related component or system failures or anomalous events that have occurred in the past and are associated with a given hazard cause or failure mode.

D.2.1.6 OPERATING & SUPPORT HAZARD ANALYSIS

The general purpose of the O&SHA is to perform a detailed safety risk assessment of a system's operational and support procedures. Mission Operations-related data will be provided as part of the Phase I and subsequent Hazard Analysis. The O&SHA identifies hazards and recommends risk reduction alternatives in procedurally controlled activities during all phases of intended system/hardware/software/facility use.

The O&SHA examines human induced hazards to hardware, software, equipment, and facilities and how the hardware, software, equipment, facilities, and environment can create hazards for humans. Generally, the O&SHA examines those operations that are procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons and equipment and consider:

1. Planned system configurations at each phase of activity - Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risks during these activities. These activities should be analyzed to provide preventive measures to reduce the hazard to an acceptable level.
2. Facility interfaces - Potentially hazardous conditions that may be induced into flight hardware during manufacturing, test, inspections, ground operations, etc., and then show up later during flight hardware/software end use. These

- D-11 conditions should be analyzed, and appropriate mandatory verification points implemented. (Included are such items as poor welding, unidentified hardware failures, x-ray effects on electronics, and contaminated fuel.
3. Supporting tools or other equipment specified in use - Such as safety devices and equipment, including personnel safety and life-support equipment (i.e., PPE).
 4. Operation or task sequence, concurrent or parallel task effects, and limitations.
 5. Biotechnological factors.
 6. Regulatory or contractually specified personnel safety and health requirements.
 7. Potential for unplanned events, including hazards introduced by human error, warnings, cautions, and special emergency procedures ((e.g., egress, rescue, escape, render-safe, and back-out).
 8. Changes needed to support functional or design requirements for system hardware and software, facilities, tooling, or support/test equipment to eliminate hazards or reduce associated risks. These changes will be analyzed to verify effectiveness of implementation.
 9. Handling, storage, transportation, maintenance, and disposal of hazardous materials. These requirements should be analyzed, and proper requirements and procedures implemented.

The O&SHA documents system safety assessments of procedures involving system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, and disposal. An O&SHA recommended format and data elements may be found below in Table D.2.1.6-1. The O&SHA is developed with the intent of establishing a systematic review and documentation where the operations are broken down into incremental parts and consistently analyzed for hazards.

TABLE D.2.1.6-1 O&SHA FORMAT AND DATA ELEMENTS

O&SHA NO.		ENGINEER:	
OPERATION:		DATE:	
TASK:			
SUBTASK:			
STEP			
CRITERIA/CONSTRAINTS/ ENERGY SOURCES	(Identify operational constraints and criteria such as: voltage levels, pressure ranges and frequency. Identify presence and quantities of energy sources such as fuels, propellants, pressure vessels, explosives, batteries.)	SHEET	1 of 1

D-12

HAZARD	HAZARD CAUSES	HAZARD EFFECT	SEVERITY LEVEL	SAFETY REQUIREMENTS	HAZARD RISK ELIMINATION / CONTROL PROVISIONS	VERIFICATIONS	LIKELIHOOD OF OCCURRENCE
Describe the hazard created by or during the operation including the scenario and hazardous events that must be controlled	Describe the mode(s) of failure or processing induced conditions (Refer to SSHA instructions)	Describe the potential effects or impact on personnel and equipment	Identify the worst-case severity as one of the following for each hazardous condition: Catastrophic, Critical, Marginal	Describe recommended measures for preventing, eliminating, or controlling the hazardous condition. Include guidelines, recommended design or operational requirements, and recommended further analysis or actions	Identify proposed hazard reduction methods for open hazards and implemented reductions for controlled hazards	Identify the methods used to verify the hazard controls. Include sufficient detail/ explanation of testing, inspection, and analysis, which control the hazard and support hazard closure or risk rationale. Verification acceptance methods include analyses, tests, inspections, and demonstrations. Identify the verification reference by document number and title.	Assess the controls that are in place and determine the hazard likelihood after the controls are applied. The likelihood justification includes the associated uncertainties or confidence factors. State likelihood in these terms: Very High High Moderate Low Very Low

D.2.1.7 SOFTWARE HAZARD ANALYSIS

Software safety is the safety-critical software aspects of system safety. Software safety is a system issue and will be analyzed from a system context. Software safety analyses are initiated in the Concept Development Phase, matured through the Preliminary and Final Design phases, verified in the Fabrication, Assembly and Test phase and maintained in the Sustaining Phase. The software system should be designed, developed and tested to 1) prevent hazardous software behavior, 2) reduce the likelihood of hazardous software behavior, and 3) mitigate the negative effects of hazardous software behavior.

NOTE: For the purposes of this document, firmware is considered software.

The function of software safety is to derive the software safety requirements, analyze the software design, software code implementation, and the software and system test results where safety-critical software is validated or verified. The results of these analyses should be documented in the phased SDPs.

The software safety function is initiated in the Concept Development Phase with the identification of safety-critical software functions. Software safety analyses should take place during all phases of system development and the results should be incorporated into the SDPs delivered at the design milestones.

Software is safety-critical if it meets at least one of the following criteria:

- a. Resides in a safety-critical system (as determined by a hazard analysis) AND at least one of the following:

- D-13
- Causes or contributes to a hazard.
 - Provides control or mitigation for hazards.
 - Controls safety-critical functions.
 - Processes safety-critical commands or data.
 - Detects and reports, or takes corrective action, if the system reaches a specific hazardous state.
 - Mitigates damage if a hazard occurs.
 - Resides on the same system (processor) as safety-critical software and is not logically separated from the safety-critical software.
- b. Processes data or analyzes trends that lead directly to safety decisions (e.g., determining when to turn power off to a wind tunnel to prevent system destruction).
- c. Provides full or partial verification or validation of safety-critical system, including hardware or software subsystems.

The Software Safety Design Analysis:

- Ensure the software safety requirements are correctly incorporated into the software design.
- Ensure that the software design clearly identifies the safety design features (e.g., inhibits, failure detection and recovery, assertions, etc.) that are used to implement the software safety requirements.
- Ensure that the partitioning or isolation methods used in the design isolate the safety-critical design elements from the non-safety-critical. This is particularly important with the incorporation of COTS software.
- Ensure that the software design is evaluated for the following:
 - Failure of the software to perform a required function,
 - The software performs a function that is not intended,
 - The software possesses timing and/or sequencing problems,
 - The software fails to recognize that a hazardous condition occurred and fails to initiate the appropriate response,
 - The software produced the intended but inappropriate response to a hazardous condition. Software may be developed “correctly” with regard to the specification, but wrong from a systems perspective due to misinterpretation of intent.
 - Vulnerabilities to operator error and operator required monitoring, diagnosis, and actions for hazard control,
 - Response time and capacity/throughput, including max loading conditions,

- D-14
- Best case and worst-case execution time,
 - Deadlock and livelock, and
 - Overflow and underflow of data.
 - Software self-monitoring and exception handling
 - Monitoring of electronic hardware
 - Diagnostics and periodic testing (RAM check, code space checks, hardware excitation checks)
 - State transitions are defined such that unacceptable states are prevented or addressed.
 - Single point failures which could result in the loss of safety-critical functionality.
 - Ensure that the safety-critical design elements are traceable to the software safety requirements. Without adequate, correct, and complete safety requirements, the system behavior is at risk and may result in a hazard.
 - Ensure compliance to the software coding standards.
 - Ensure that the software safety requirements have been implemented in the code as intended.
 - Ensure that the code implementation does not compromise any safety controls, does not introduce any other potential safety concerns, and maintains the system in a safe state during all modes of operation.
 - During the operations and maintenance phases, when software changes are made, all of the previously described analyses are applicable during software development.

D.2.1.8 DESTINATION PROVIDER INTEGRATED HAZARD ANALYSIS

The Destination Provider is the integrator of the hazard analysis provided by other affected Commercial Providers, transportation systems, and end items interfacing with the Destination environment or systems. The transportation systems, interfacing end items, and Destinations are responsible for identifying hazards, hazard controls, and verification methods and status, as well as Destination and flight crew survival capabilities and emergency response procedures and analyses for the design life of the item under examination. The hazards and emergency response capabilities should be identified using the methodology defined in this document, recorded in HRs, and maintained for the life of the system.

D.2.1.9 INTEGRATED HAZARD ANALYSIS

Integrated Hazard Analyses (IHAs) provide a top-down assessment of hardware, software, and operational interactions that identifies both the hazards that can result from those interactions, as well as how those hazards are controlled. IHAs include those cases for which multiple modules, utilization, cargo, and/or transportation systems

D-15 provide controls. IHAs ensure that interactions across interfaces do not create a hazard. An integrated hazard is defined as a hazard that:

- A. Impacts causes/controls/verifications to the interfacing hardware and/or operating environment,
- B. Relies on upstream services for a level of control (e.g., bonding to vehicle structure, electrical power removal, etc.), and/or
- C. Associates with the interaction between two or more end items, modules, or vehicles.

It is recommended to identify integrated hazards early in the safety review cycle, beginning with the development of the PHA. This method ensures overall program risk is addressed at a point in which appropriate design controls can be considered without major cost or schedule impacts, incorporating and confirming the hazard control strategies agreed upon with other affected Commercial Providers (refer to Table D.2-1 in Appendix D.2, Hazard Analysis Types).

The Destination Provider is the integrator of the hazard analysis provided by other affected Commercial Providers. The affected Commercial Providers' HRs should cite the relevant integrated HR as a cross-reference. The integrated SDP should be addressed as early in the phase review cycle as possible (refer to Table 4.0-1, Safety Milestones and Development Schedule). Hazards associated with the interaction between two or more end items or modules are addressed in an integrated assessment and/or HR.

D.2.1.9.1 ROLES AND RESPONSIBILITIES

Negotiations between Destination and Transportation Providers should begin at the start of the lifecycle to establish roles/responsibilities of all the interface Commercial Providers early in the developmental process. A responsibility matrix, as shown in Table D.2.1.9.1-1, Responsibility Matrix, outlining the hardware, interface, and responsible parties, can help facilitate these conversations.

TABLE D.2.1.9.1-1 RESPONSIBILITY MATRIX

HARDWARE	INTERFACE	RESPONSIBLE COMMERCIAL PROVIDER FOR SAFETY ASSESSMENT

Hazardous conditions caused by one system/end item require hazard controls external to that Commercial Provider's end item. The overall design philosophy is to achieve efficient design and avoid duplicate or unnecessary hazard controls on both sides of an interface. When hazard controls are distributed across an interface, the following are used:

- A. The affected Commercial Provider should discuss and propose allocation of hazard control responsibility. In cases where there may be cost or schedule

D-16 impacts, elevated safety risk, or technical disagreement, the hazard control strategies should be discussed with the appropriate SRB as early as possible for resolution of issues and concerns. Additional information regarding the appropriate SRB roles and responsibilities can be found in Section 5.0, Safety Review Roles and Responsibilities.

- B. The functionality, capability, or physical requirements for hazard control are documented in Interface Requirements Documents (IRDs), Interface Control Documents (ICDs), design specifications, or other appropriate bilateral requirements documents and documented in Commercial Provider HRs.

The Destination Provider integrated HRs should reflect the complete and integrated hazard control strategy for each hazard, incorporating and confirming the hazard control strategies agreed upon with affected Commercial Provider.

D.2.1.3 MAINTENANCE HAZARD ASSESSMENT DURING ON-ORBIT OPERATIONS

MHAs identify applicable hazard controls from baseline HRs, documents an analysis to determine if any new hazards are present during the maintenance activity, and captures new hazard controls in a new MHA HR. This MHA HR may cover multiple types of hazards rather than writing a new HR for each type of hazard (such as sharp edges and electrical hazards may both be present in the same MHA HR under different causes). If no new hazards are identified, then the MHA will not need a new HR. The MHA should be addressed as early as possible in the phase review cycle, starting with a preliminary assessment at Phase I (refer to Table 4.2-1, Safety Milestones and Development Schedule).

MHAs are a critical element in the removal and replacement of hardware and include the following:

1. **Safe Access** - This assessment addresses all potential access paths for contact hazards (for example, sharp edges, accessibility, touch temperature, stored energy, and electrical shock, toxicity assessment, material release) that may be present during maintenance activities.
 2. **Modification of Existing Safety Features** - This assessment addresses hazards that maintenance activities can create (for example, contamination). This includes establishing why the maintenance tasks are safe to perform and why it is acceptable to temporarily bypass any hazard controls during maintenance activities.
- A. **Temporary Loss of any Critical Items, Subsystems/Systems during Planned Maintenance Outage** - This assessment addresses hazards that maintenance activities can create from requiring temporary loss over worst-case planned duration for Temporary Loss of any critical items, subsystems/ systems during planned maintenance outage. Examples include environmental control and life support or warning or control system impacts, etc.

D-17 **Reverification of Safety-Critical Features** - This assessment addresses the approach to verification or reverification of safety-critical features that may be modified during maintenance and that will be required during subsequent operations.

D.3 HAZARD SEVERITIES/LIKELIHOOD

Hazards are categorized in accordance with their hazard severity/likelihood levels and the ratings are documented in a hazard scoring matrix. The residual risk posture for each hazard is defined in subsequent levels of elevated risk acceptance reporting as defined in Table D.3-1, Elevated Risk Acceptance Reporting.

An example of a hazard scoring matrix is provided in Table D.3-2, Hazard Scoring Matrix Example.

TABLE D.3-1 ELEVATED RISK ACCEPTANCE REPORTING

Red	HRs including residual risk require approval by the NASA Administrator
Yellow	HRs including residual risk (Program Level Risks) require approval by Program Control Board(s)
Green	HRs including residual risk (Equivalent Safety Risks) require approval by the safety review board co-Chairs

TABLE D.3-2 HAZARD SCORING MATRIX EXAMPLE

Likelihood	Very High	N/A	N/A	N/A		
	High	N/A	N/A	N/A		
	Moderate	N/A	N/A	N/A		
	Low	N/A	N/A	N/A		
	Very Low	N/A	N/A	N/A		
		Minor	Moderate	Severe	Critical	Catastrophic
		Marginal				
		Severity				

D-18 D.4 EMERGENCY RESPONSE

D.4.1 EMERGENCY RESPONSE PROCEDURES

Emergency response and associated planning, including procedures, PPE, and emergency response hardware/systems (Patch kits, defibrillator, smoke remediator, clean up kits, etc.) add robustness to the Destination design and provide the ability to interrupt the progress of a hazard sequence preventing a loss of crew event and/or allowing the recovery of the Destination/transportation systems from a catastrophic event.

D.4.1.1 EMERGENCY RESPONSE EQUIPMENT AND SYSTEMS

Performing an HA on emergency responses is scoped by using identified emergency scenarios and procedures and includes related emergency equipment (PPE, fire extinguishers, smoke remediator, leak detectors, etc.). Emergency equipment and systems is defined as a set of components (hardware and/or software) used to mitigate or control hazards, after occurrence, which present an immediate threat to the crew or crewed spacecraft. Emergency equipment and systems (e.g., fire extinguishers, breathing masks) reside in the crew accessible locations when not in use and during crew use.

D.4.1.2 CREW SURVIVAL METHODS

Based on trade studies/analyses, the crew survival capabilities available and implementable during each phase of the mission will be determined. Incorporating and preserving the capability for the crew to safely return from the mission is a fundamental tenet of human-rating.

The broad strategies and the process used to develop the strategies that respond to the scenarios help to establish a focus of making crew survival an integral element of the design process. Continued challenges to (and deliberations concerning) the scenarios themselves and the assumptions, analyses, and design decisions that flow from these scenarios are essential to successfully obtaining Human-Rating Certification.

D.5 COMPUTER SYSTEM SAFETY

Software malfunctions that are the result of external causes (i.e., hardware faults or firmware flaws) can usually be isolated to a specific device and are detected by such means as Built-In Tests, Fault Detection, error handling, self-checking logic on multiple processors and output voting used with redundant computer sets.

Standard types of malfunctions include:

- Software malfunctions that are the result of internal causes (like software faults) would be controlled through well-structured software lifecycle, management, and security efforts.
- Software malfunctions that are the result of erroneous commanding (including updating, patching, or memory modification) should be controlled with a detailed strategy for how to execute hazardous commands, encryption,

- D-19 processing/validation, checksums. This should be accompanied by analysis for prerequisite checks, hazardous commands issued out of an automation (sequence or failure recovery), and monitoring for the execution and command response).

The following are examples of common cause failures:

- a. A design deficiency,
- b. An operator error,
- c. A human-induced event,
- d. A natural phenomenon, or
- e. An unintended cascading effect from other operation or failure within the system.

The following is an example of a common mode failure:

- a. Computers or avionics built with a systemic error.

The following are examples of software common mode failures:

- a. Latent or misconfigured operating system error
- b. Task overrun
- c. Stack Overflow
- d. Operating system
- e. Logic code, and
- f. Other failure modes for avionics, referenced in NESC-IB-24-01986

It should be noted, diversity reduces the potential for common mode failures, but it does not eliminate the potential for common cause failures.

D.5.1 BLACK OUT ZONE ANALYSIS

Software BOZ analysis for fail silent scenarios assesses each safety critical system to assess the system response if all the software outputs cease. For example, a cabin vent valve that remains in the last commanded state could cause a structural hazard and a toxic environment hazard. BOZ analysis for erroneous outputs is more difficult. It is not expected to analyze all possible software outputs for the entire mission. It is expected that short time to effect hazards where recover/repair is not an option are analyzed for robust designs (e.g., dissimilar redundancy, inhibits, prerequisite logic, interlocks).

Examples of such short TTE failures are loss of control during dynamic phases of flight, ordnance events, mechanisms, propulsion pressurization, and power switching. If any scenarios are identified in which a software common cause/mode failure will cause a

D-20 catastrophic hazard (despite system redundancy or operational mitigations), this scenario is designated as a BOZ and will need risk acceptance.

It is probable that the BOZ analysis is not clear cut, and a catastrophic hazard may occur. In this case, the scenario and likelihood should be assessed by the safety board where it will be decided if the failure tolerance requirement has been violated and how best to identify and address the risk.

D.5.2 COMMON CAUSE/MODE FAILURE CONTROL STRATEGY AND RISK MITIGATIONS

System design accounts for common cause/mode failure (See a. System Failure Tolerance, below). In this situation, hazardous behavior remains controlled in the event a common cause/mode failure occurs. One option for potentially restoring complete functionality may be to restart one or more flight computers. Depending upon the mission phase in which the fault is encountered, this recovery operation may exceed the TTE for catastrophic hazards or depending on the failure mode, may not restore functionality. Another process and design mitigation is to recover and/or repair the software and system state (i.e., be updating the flight software image(s) (See b. Recover/Repair).

The following is a detailed description of the two strategies used to control and mitigate software common mode failures, as well as risk mitigation activities implemented during the Software Development Process:

a. System Failure Tolerance

- What - A system design that provides independent controls to the hazard such that a software common cause/mode failure does not lead to the failure of more than one hazard control
- When to use - Whenever possible, this is the preferred strategy. Providing a fully functional redundant set of capabilities to avoid a catastrophic hazard (which may include dissimilar software) is viewed as an equivalent risk and meets the intent of failure tolerance requirements.
- How to Implement
 - Incorporate dissimilar redundancy (fault down/safe-mode embedded software, backup systems – based on separate requirements, minimize shared code) within the system to completely control the respective catastrophic hazard, and architecture (partitioning of flight critical software from non-critical software)
 - Document as control(s) in respective HRs with appropriate verifications
 - Examples:
 - Implementation of a subset of critical vehicle system functions by dissimilar software, hardware, or combination of hardware and software
 - Isolate and distribute software functions through such technologies as distributed network based architectures or virtual partitions

- D-21
- Provide capabilities for the vehicle to avoid catastrophic hazards by being able to safely operate in a limited or degraded state
 - Provide capabilities for the crew to bypass software functions and manually control flight systems/actuators

b. Recover/Repair

- What - Process and design control to recover and/or repair software and system after software common mode failure occurs before a catastrophic hazard is realized. During recover/repair, the fault is corrected or mitigated, and critical functions restored.
- When to use
 - “a. System Failure Tolerance” is not achievable.
 - Detection and recovery of the failure is within the time to criticality before a catastrophic hazard occurs.
- How to Implement
 - The analysis performed must show that the recovery/repair (reboot and recover, hold points, monitoring and passive aborts) can be successfully executed prior to the catastrophic hazard TTE
 - Document recovery/repair plan and supporting design features if applicable in the respective HRs with appropriate verifications
- Examples:
 - Reboot and reinitialize, system watchdog function
 - Runtime software audits that repair damaged data structures
 - ‘Fault-down/safe mode’ embedded software
 - Passive aborts
 - Backup Systems (based on separate requirements, no shared code)

These hazard control strategies and mitigations should be presented in hazard space per mission stage, phase or mode. If system failure tolerance cannot be achieved, a risk acceptance or Safety Non-Compliance/Variance in accordance with Section 3.3, Safety Non-Compliance/Variance, is required to characterize the risk with applicable time/flight phase and provide flight rationale for acceptance.

Even with rigorous software development processes with an extensive verification and validation campaign, past missions have shown that common cause/mode software failures can and do occur.

D.5.3 SOFTWARE CONTROL AND MITIGATION BEST PRACTICES

The Commercial Provider Safety organization and the Commercial Provider Software organization should work together to ensure HR controls are properly verified. Proactive involvement not only supports a check and balance between Safety and Software but ensures test plans/procedures and success criteria are written and executed not only to close requirements but to accommodate hazard analysis. Testing should not just focus on closing the requirement but should fully exercise logic/code paths, test out all permutations, and include negative or stress testing (see Best Practice 2) to tease out any unexpected behaviors.

D-22 The software HR should be written in defense of software common cause/mode. As stated in Section 3.1.6, Computer System Safety, common cause/mode failure violates the catastrophic hazard requirement. Controls are written to minimize the risk. System failure tolerance is a control strategy. A process and design mitigation is to recover and/or repair the software and system state. Analysis for TTD/TTE and BOZ will indicate where hazard controls and mitigations are not sufficient to prevent a catastrophic event. The remaining risk will need to be characterized and documented in a Non-Compliance/Variance.

For the appropriate SRB to recommend approval of a Non-Compliance/Variance for common cause/mode failure, the best practices listed below should be considered by the Commercial Provider. Each of these items includes aspects to be enforced throughout the software lifecycle or provide compatible alternatives that meet the intent.

1. Rigorously enforced coding standards as demonstrated by objective evidence gather by Software Quality Assurance (SQA) with the following characteristics: Industry recognized, verifiable by static analysis, mandatory inspection points, and code audits for legacy software. The coding standards should be supplemented with the appropriate CBCS requirements called out in CLDP system specification requirements, including anomaly recovery, safe termination/initialization, and input validation.
2. Utilization of static code analysis tools to verify compliance with coding standard. Utilization of code path analysis tools and reports results for critical phases (blackout zones). Code paths that are not covered should be identified and explained. Assessments of additional analysis and testing strategies that can be applied to blackout zones. Examples include Parameter Value Coverage, mission duration testing, stress, Monte Carlo, and performance end-to-end testing. Also, ensure appropriate task priorities are in-place (e.g., Guidance, Navigation and Control (GNC) should be higher priority than non-safety critical tasks and fault response sequencing should be in order of severity). In these cases, engineering judgement is expected on what types of duration would be value added.
 - a. Mission duration testing is valuable to identify memory management efficacy, unexpected counter overflows, and ensuring limit checks are appropriate.
 - b. Stress testing: Inserting multiple failure modes of sensor/effectors, failing strings, artificially causing memory leaks, CPU overruns, excessive bus bandwidth loading, software exceptions (common cause/mode, across all flight computers). Artificially causing jitter in clocks/sync algorithms. Design the tests so they can be used for flight-to-flight regression testing. This should also include robust negative testing.
 - c. Test bed model validation: Identify a process where simulation models are certified/validated for use in verification of flight software. Compare models with real data where available. Incorporate highest available hardware (i.e., flight equivalent unit) in test beds. If possible, utilize separate simulations/emulators to compare results. Where feasible,

- D-23 incorporate tools that allow for self-checking of test results (pass/fail). Use of such tools should also be validated.
3. Implement a clearly defined software severity classification system for all software non-conformances that could impact flight safety (including tools and applicable ground systems). At a minimum, classes should include loss of life or loss of vehicle, mission success, visible to the user with operational workarounds, and an 'other' class that does not meet previous criteria.
 - a. Commercial Providers should clearly define and identify their 'safety-critical' software (NASA-STD-8739.8, NASA Software Assurance and Software Safety Standard Section 4.2 Safety-Critical Software Determination) and are strongly suggested to list rationale for their classification (i.e., tied to a particular HR, processes hazardous commands).
 - b. Changes, including safety critical data, high severity non-conformances and new capabilities that have the potential to impact Flight Critical software, should require formal board approval led by the Commercial Provider's management with representatives from Software Development, Test, Requirements, Software Safety, Operations, Independent Verification & Validation (IV&V).
 - c. Mandatory assessments of vendor reported defects for all COTS/Modified-off-the-shelf (MOTS) based software that have a direct impact on Flight Critical Software.
 - i. This includes Operating Systems, run-time systems, flight-critical device drivers/firmware, code generators, compilers, math libraries, IT security vulnerabilities, build and configuration management tools. These assessments are to be performed pre-flight, with mandatory code audits for critical defects.
 4. Mandatory process assessments for all high severity safety-critical software issues (closed loop process). For high severity process escapes, identify the earliest process step where the escape could have been identified and all subsequent steps including steps beyond where the escape was discovered and determine what process step update(s) are needed to preclude such an escape at that step(s) again. The rigorous process with corrective action feedback needs to be in place at initial code development with evidence of effective process changes no later than the required NASA software quality assurance audit. In progress development requires a legacy code audit by the Commercial Provider.
 - a. Mandatory code audit assessments for all high severity software issues; determine where similar escapes could have occurred, define audit criteria, perform audit and share results with CLDP.
 - b. Collect metrics with objective evidence demonstrating that over-time escapes are being caught earlier in the development process and that the process modifications are effective.
 - c. IV&V provider must assess their own escapes to determine similar process changes.

- D-24⁵. Independent Moderator role: For all critical code reviews and requirements change processes, have a separate reporting chain to ensure an independent review of the compiled data (can be an internal SQA person).
- a. Recommend formal peer reviews for requirements changes/flow down. Incorporate checklists in requirements, code, and test script peer reviews. Maintain record of checklists for audit purposes. Recommend using an independent moderator to ensure peer reviews have appropriate subject matter expert (SME) personnel in attendance, checklists are addressed, and actions addressed/closed.
6. Implement clearly defined quality and performance software metrics.
 - a. Metrics should provide management with an assessment of the quality of the software development processes. (e.g., are we getting better (fewer errors), worse, or about the same). Metrics should also consider the severity of the issues.
 - b. Performance metrics should include processor and memory utilization, network/comm path loading, transport lag, peak, and margin measurements.
 - c. The Commercial Provider reports, as a recurring stage-by-stage and/or flight-by-flight verification, metrics supporting compliance with the processes established in the HR. For identified deviations or escapes from these processes, the Commercial Provider should provide a corrective action plan that will prevent recurrence of the identified process failure.
 7. For software issues discovered after verification testing has been initiated, or on a released flight software product, completion of the analysis and flight rationale is required prior to stage/flight readiness review milestones. Issues after this point should be reported and worked as part of the mission operations functions.
 8. Define and provide a design strategy to assure control for the occurrence of a common cause/mode error. Implementation needs to be able to handle transient errors and preclude the manifestation of cascading failures in the case of non-transient errors and ensure software can be recovered regardless of the faulted state. Strategies should address items such as task restart, exception handling, potentially on an operational phase basis. This should be addressed as part of your process implementation (Implementation of NPR 7150.2 [SWE-134] 3.7 Safety-Critical Software and CLDP-REQ-1130 - Recovery for CBCS Anomaly).
 9. Identify software security requirements and associate them with security controls consistent with the needs of the supporting system, as defined in NPR 2810.1, Security of Information and Information Systems, and FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, to help ensure that software is built and deployed in a secure manner.
 - This includes access controls to restrict users to proper levels of access / user privileges, utilizing protection mechanisms, such as encryption, for the transmission of sensitive information, and controls to detect potential malicious activity that could result in a functional failure or mishap.
 10. Where hazard controls are expressed or implemented by configuration data, the data will be:

- D-25
- Expressed in terms of permitted range and authorized combinations of its operational parameters (where applicable)
 - Compatible with the underlying software

D.5.4 SOFTWARE SAFETY HAZARD ANALYSIS

The safety HA process ensures that all computer systems or any system that involves software as a hazard cause or used as a hazard control means has an acceptable level of risk. The software safety hazard analysis assesses for all safety-related hazards that are caused by malfunctioning, error coded, or non-functional software (i.e., failure modes due to all variations of software common cause/mode failures) throughout all mission phases and operational scenarios. The Commercial Provider is responsible for evaluating and documenting the necessary controls and verifications in a HR and provide a CBCS compliance matrix to be reviewed by the Computer Safety Panel prior to Phase I, II and III.

D.6 HAZARDOUS MATERIAL CONTROL STRATEGY

D.6.1 HAZARDOUS MATERIAL SUMMARY TABLE

The HMST is a listing of all identified hazardous materials that is tracked through the development and launch of the end item. Once manifested for a flight, the HMST is tracked as part of the flight specific HMST and then the on-orbit HMST. The HMST is used to identify materials in the event of an inadvertent leak or release of hazardous materials. The HRL and any special notes and comments captured in the HMST identify how to respond appropriately.

Printed or electronic copies of the relevant pages of the HMST are provided to payload, system, or GFE hardware customers and an appropriate review board to support safety assessments for payload hardware. After verification, the final HMST is provided to flight controllers and other mission support personnel. The appropriate sections of the HMST for a particular mission are provided to the utilization, system, or government furnished equipment (GFE) organizations, as needed, to verify the accuracy of the information on the chemicals or biological materials that they intend to fly. It is used to verify sample loading prior to hardware turnover for pre-launch stowage in spacecraft. Before a spacecraft launch, the data from the HMST for that mission are transferred to mission-specific electronic files, which are provided to mission support personnel for loading onto the onboard computers and the flight controller's computer in the Mission Control Center to provide real-time toxicological support.

CLDP-STD-3102 Baseline - DRAFT

D-26

Bio_ECLSS_Tox_Submittal, Version dated 02/04/2019

Please complete each field below and all applicable tabs. Place and hold cursor over boxes with red triangles for detailed instructions. Please submit completed form by email to: jscbio-ec@clsc.com

Date submitted:	
DATE HMST NEEDED (At least 2 weeks past date submitted):	
Name and number of experiment or hardware:	
Acronym:	
OptHom:	
ISS Hazard System (IHS) record number:	
Kit-level / Assembly-level part number and name:	
ISS Module (storage):	
ISS Module (use):	
International partner concurrence?	
Does this experiment involve thermal heating or combustion (e.g. furnace)?	
Is information proprietary? If so, please read note	
Principal Investigator name, title, and affiliation:	
Contact person:	
Address (building and room number):	
Phone:	
Fax:	
e-mail:	
Targeted Mission:	
Previous mission information:	
Brief summary of the experiment or conditions of use including process conditions (attach additional sheets as necessary):	

Note: Per JSC 27472 - Requirements for Submission of Data Needed for Toxicological Assessment of Chemicals to be Flown on Manned Spacecraft, data submission is required for all Programs, including, but not limited to, ISS, CC9, MPCV, and Gateway. This distribution list/mailbox has a limited, protected distribution to only authorized NASA specialists responsible for reviewing the submitted data for toxicology, biological safety, and ISS environmental control/life support system impacts. Based upon review/conclusions from these specialists, a flight safety Hazardous Material Summary Table (HMST) will be prepared and provided back to the submitter for inclusion of this HMST within their flight safety data package. If any information within this form is considered proprietary/limited rights, then the submitter shall clearly identify or label any information as such within this form and within the transmittal email subject and body. If necessary, this file may also be password protected prior to submittal, with the password sent via separate email or via other methods (as coordinated with NASA specialists).

The following section is to be completed for non-biological components, including all liquids, gels, particles, or gasses contained in the payload or system.

ID Label	Chemical / Reaction Product	Experiment Subsystem	Part # of Subsystem	Maximum Concentration	Maximum # of Samples	Maximum Amount / Sample	pH of Solution	Particle Size or Size Range	Sample Surface Area	Vapor Pressure, Partial Pressure, and Volume of Gas	Solubility in Water and Henry's Law Constant	Thermal Stability	Known Reactive Hazards

If investigator has obtained experimental results indicating the amount of sample vaporized, JSC Toxicology will accept those data to inform their toxicological assessment. If such results do not exist or cannot be shared, please include the requested information about the proposed experiment below so that JSC can calculate a worst-case vaporization amount.

Metal Component	Atomic Weight (g/mol)	Metal in Alloy (%)	Sample/Metal Weight (g)	Vapor Pressure (mmHg)	Processing Temp. (C)	Processing Time (sec)

The following section is to be completed ONLY if recombinant DNA or RNA will be used.

Identification of Material	Origin of Biological Material	Recombinant DNA or RNA	Type(s) of Vectors and Viral Replication Capacity	Use of Defective DNA/RNA with Helper Virus	Size of Insert/ Total Genome	Nature of Inserted Sequence	Inserts Codes for Known Oncogene or Toxin

Integration of Inserted DNA into Host Genome	Protein(s) Produced	Type(s) of Host	Alteration of Host Range Resulting from Research	Enhancement of Agent Virulence	Research Effects on Agent Transmissibility	Staff Training for Safe Handling of Agent	Medical Surveillance Requirements/ Recommendations	Immunization Requirements/ Recommendations

FIGURE D.6.1-1 HAZARDOUS MATERIAL SUMMARY TABLE

In addition to the documents and forms above, phase safety data submittal checklists are available as another tool to assist the Commercial Provider to ensure all technical data for any phase has been submitted to various engineering technical disciplines and the boards to support hazard controls and verifications.

D-27 **D.6.2 BIOLOGICAL MATERIALS**

The following historical BSL ratings are provided for reference. References for samples collected in-flight are specific to crewmember sampling only.

1. Human cell lines are generally rated as BSL-2M based on information contained in the 5th edition of "Biosafety in Microbiological and Biomedical Laboratories" published by the CDC and NIH. The rating will be higher if the human cells are determined to be a higher risk.
2. Waste from SPF rodents is assessed as BSL-1.
3. Blood samples collected in-flight are assessed as BSL-1.
4. Saliva samples collected in flight are BSL-1.
5. Urine samples (freshly voided, treated with disinfectant/preservatives, or frozen) collected in-flight are assessed as BSL-1. Urine samples (not treated with disinfectant/preservatives and stored at ambient temperature or refrigerated for more than 24 hours) collected in flight are considered BSL-2M.

D.6.3 ECLSS HARDWARE AND CABIN ENVIRONMENTAL IMPACT

The ECLSS E Ratings and THL are generally considered to be independent of one another with one exception; when interaction with the ECLSS hardware or environment results in chemical reactions and additionally hazardous chemicals. This would be the case when a chemical thermally decomposes upon exposure to the ECLSS hardware processing temperatures, moisture is present in the cabin atmosphere, and/or the condensing heat exchangers to produce products are more harmful than the flown chemical. Any potential products from interaction with ECLSS hardware is provided to the toxicologist for consideration when assigning the THL rating.

The potential hazards from mixtures of chemicals, chemical reactions, and thermal decomposition products should be assessed as necessary.

D.6.4 PHYSICAL AGENTS

Physiological Hazards

The unique attributes of the decreased gravitational environment cause particles to remain suspended in the air for extended timeframes. The main physiological hazards caused by particle release for the crew are suffocation and asphyxiation. Particles > 10 µm in diameter released in large amounts cannot be inhaled deeply into the lower respiratory tract (lungs) but could cause acute asphyxia (suffocation within a few minutes) due to mechanical blockage of the upper respiratory tract, especially the larynx. Particles ≤ 10 µm diameter can be inhaled deeply into the lungs and cause a slow asphyxiation (suffocation within many minutes to hours) by obstructing the deep lung and interfering with oxygen exchange.

Concentrations below occupational limits are considered acceptable as they are not expected to cause any significant hazard or permanent health issue. Control to prevent release is not required but remains recommended when feasible. The release of

D-28 particles in this size and concentration are considered as a nuisance and will be indicated as such on the HMST.

Shatterable Materials

Shatterable materials are unique physical agents. A shatterable material is any material that can fracture under a load or impact and produce fragments that are potentially hazardous to the crew and/or vehicle. Common shatterable materials may include glass, ceramics, display monitors, certain metallic alloys, optical equipment, frangible, and any other shatterable materials that can fracture and produce fragments. Shatterable materials can potentially cut/damage the eye or skin and contaminate the environment and pose an asphyxiation risk.

Release of shatterable materials, inert sharp particles, $> 50 \mu\text{m}$ in their longest dimension are considered a catastrophic hazard due to the potential to cause a disabling injury, even after a brief exposure. Shatterable materials $\leq 50 \mu\text{m}$ are typically considered acceptable, however, they can present a potentially catastrophic hazard if released at high velocity and are assessed on a case-by-case basis.

The control strategy for shatterable materials often relies on a DFMR philosophy with appropriate verifications rather than failure tolerance, as applying failure tolerance can be a challenge for many of the applications where shatterable materials are used.

Shatterable items may be used open cabin after an inspection through a clear bag or through a protective device. The items often must be placed back in a bag or protection when not in use.

Consideration should also be given to implementing the Occupational Health and Safety Administration (OSHA) recommendations that work with nanomaterials occurring in ventilated enclosures (e.g. glove box, laboratory hood, or process chamber) equipped with High Efficiency Particulate Air (HEPA) filters.

D.7 HAZARD CONTROL ORDER OF PRECEDENCE

ELIMINATE THE HAZARD

The primary method (and preferred first choice) for reducing hazards is through a design approach that prevents the occurrence of the hazard. Hazard elimination is accomplished by eliminating the hazard source by deleting (e.g., selecting non-hazardous sources of materials) or eliminating the hazardous operation (e.g., selecting a design that achieves its purpose using non-hazardous operations).

REDUCE RISK THROUGH DESIGN ALTERATION

When elimination is not possible, control and isolation of potential hazards and FT considerations should be included in design approach using the following methods:

- a. Incorporate design features or devices, that, if implemented correctly, would prevent the hazard (e.g., FT inhibits, FT/redundancy of critical functions, etc.).

- D-29^b. Design changes that reduce the severity and/or the likelihood of the hazard(s) (e.g., increased high margin to design factors of safety to failure or substitution of less hazardous technologies/substances/energy sources).

USE OF OPERATIONAL CONTROLS

Where it is not possible to reduce the hazard by design, real-time activities of the on-orbit crew, issuance of a ground command, or implementation of a preplanned decision (e.g., safety-critical flight rules) may be used to counter hazardous conditions.

Operational hazard analysis and procedural mitigation process and products allows for the operational controls to meet the intent of CLDP-STD-1150, Commercial Low-Earth Orbit Development Program Operations Standards.

Operational controls are necessary when the design solutions fail to resolve the issue, acting as a workaround executed by the crew. However, managing operational control of hazards can be difficult and may increase the risk of human error.

Operational controls should be implemented with the following precedence: (1) procedures, (2) flight rules, and (3) training. Procedures are the primary method and used for operational controls (e.g., crew close a manual valve, to provide a second control/barrier to a hazard, crew torque safety-critical fasteners to a specified torque value, ground mode a vehicle to free-drift within TTE, if automated system fails, etc.). The next method, flight rules, is normally for aspects that are not contained in a nominal procedure (e.g., thermal requirements, contingency situations, lighting). The last method of operational control is crew training. It is difficult to reliably verify that the crew understands the intent of the control and it requires proficiency/currency training to maintain the crew member's ability to perform the operation within the TTE for the hazard.

For Critical or Catastrophic hazards, the use of flight rules, procedures and training as the only risk reduction method should be avoided. The use of ground commands as operational controls is only applicable for those failures whose TTE is longer than a pre-determined maximum allowable planned outages or Mean-Time-To-Repair of the ground systems and communication links.

HAZARDOUS EFFECT MITIGATION

Where it is not possible to reduce the hazard risk of hazard occurrence to an acceptable level through design and operational controls, the use of hazardous effect mitigations allows safing and/or recovery after a hazardous event has occurred. Hazardous effect mitigations can include the use of automatic safing devices, PPE, recovery equipment, detection capabilities warning devices, and/or real-time activities of the on-orbit crew utilized to counter hazardous conditions once they occur and provide enhancements to safety.

Clear and distinct warning signals/notices and their application minimize the probability of wrong signals or of improper personnel reaction to the signal. If possible, advance cautionary notices or advisories should be utilized to prepare crew for a potential

CLDP-STD-3102
Baseline - DRAFT

D-30 associated higher-level hazard and subsequent reactive controls that may be required or occur automatically.

E-1 APPENDIX E– BEST PRACTICES FOR SAFETY DATA DEVELOPMENT

The SDP supporting documentation includes the following for the designated phases:

- Plan/Schedule,
- Target Launch and/or Destination occupancy,
- Hardware overview and description,
- Operational description,
- Planned maintenance,
- Interface description/diagrams,
- Drawings/schematics,
- Safety Commercial Provider specific requirements,
- HRs and Safety Non-compliances/Variations, as applicable,
- Crew Survival Method Documentation, and
- Supporting technical data.

E.1 HAZARD REPORTS

HRs serve as a tool for documenting controls and associated verifications to potential hazards identified in the HA, ties to related HRs, providing crucial information for overall risk acceptance. Commercial Providers identify and ensure all hazards associated with the system design, development, manufacturing/construction/ fabrication, testing, transporting, maintenance, ground safety (See Appendix K for guidelines), interfaces and operations are properly addressed, and that appropriate CSMs and/or destination survival methods are identified for all catastrophic hazards. To effectively develop a HA and associated hazard severities, Commercial Providers must have a comprehensive understanding of all end item hardware, interfaces, system boundaries, interactions, software, and planned concept of operations. Only those hazards classified as critical or catastrophic require documentation within HRs.

HRs should be standalone documents. Instead of duplicating common causes and their respective controls between HRs without providing additional insight to Commercial Provider specific requirements compliance, cross referencing is acceptable. HR supporting documentation should be submitted along with the HR to facilitate a comprehensive technical review by the appropriate SME. A list of common/standard generic hazards along with HR guidelines will be available for the Commercial Provider to use as a guide to document hazard causes, controls and verification methods based upon the hazard severity, lessons learned from previous NASA Programs, and candidate hazards in a <TBR D-1> database. The guidelines are a useful tool for performing HA and can be used as appropriate based on the system/end item design/concept of operations. Use of the guidelines by the Commercial Provider is not mandatory, however, it is a useful tool while performing HA.

F-1

APPENDIX F– BEST PRACTICES FOR PHASED SAFETY REVIEWS

F.1 PHASED SAFETY REVIEWS

The safety review process was developed to evaluate and assess the results of safety analyses conducted by the Commercial Provider. Safety compliance assessment is accomplished using a phased safety review process (Phases 0, I, II, III) that corresponds to the hardware's conceptual, preliminary, critical design, and acceptance phases (including verification/validation). The documents are provided to NASA.

F.1.1 SAFETY REVIEW AGENDA

Listed below are general agenda items for formal safety review meetings. These ensure that the safety review meetings proceed smoothly and contain the necessary information to facilitate the review. The Commercial Provider should develop an agenda that includes the following:

- A. Introduction
- B. Opening remarks
- C. Status of pre-review activities
- D. A design overview/objective
- E. An operations overview
- F. A summary of all build/test non-conformances, anomalies, and significant technical issues.
- G. Program milestone schedule:
 - 1. Design stages and reviews and corresponding safety review board dates,
 - 2. Hardware/software build status,
 - 3. Testing and verification activities,
 - 4. Delivery, integration, and launch activities.
- H. Detailed presentation of HRs (and safety non-compliances, if applicable)
- I. Verification tracking log status (Phase III)
- J. Status of safety review meeting, including newly assigned Action Items (AIs), previously assigned AI, HR and non-compliance/variance dispositions
- K. Concluding remarks

F.1.2 PHASE 0 SAFETY REVIEW

F.1.2.1 PHASE 0 DATA

If a Phase 0 Safety Review is scheduled, a Preliminary SSAR (or a tailored version of it) and PHL should be provided as part of the SDP. The safety hazard analysis process

F-1

F-2 commences in the Concept Development phase with a PHA that is documented in a Preliminary Hazard List (PHL). PHA methodology and PHL templates can be found in Appendix D.2.1.1, Preliminary Hazard Analysis (PHA).

F.1.2.2 SUCCESS CRITERIA FOR A PHASE 0 SAFETY REVIEW

The following list is provided as a reference as the type of data which may be included in a Phase 0 Review.

1. Introductions and Agenda
2. Scope and Objective
3. System Overview
 - 3.1 Organizational Structure
 - 3.2 System Description
 - 3.3 Interface Overview
 - 3.4 Operations
4. Presentation of Hazard Assessment/Analysis Approach
 - 4.1 Overview, Ground Rules, and Assumptions
 - 4.2 Hazard Analysis Approach
 - 4.3 Hazard Cause
5. Approach for Controlling Hazards
 - 5.1 FT
 - 5.2 DFMR
6. CSMs identified to extent practical
7. Special Topics (Include any Areas of Concern)
8. Forward Plan for Phase I

F.1.3 PHASE I SAFETY REVIEW

F.1.3.1 Phase I DATA

The following list of Phase I data is formally submitted 30 days, or as negotiated with the Commercial Provider, prior to the safety review and should be made available as needed for delta reviews.

1. An overview description of the design and operations of the hardware being addressed in the review, including the following:
 - 1.1 A brief description of the hardware
 - 1.2 Flight/Ground/LEO Interfaces (to another Program/Hardware/Project)
 - 1.3 Planned and proposed functions

- F-3
- 1.4 Operational scenarios related to all mission phases including maintenance and disposal
 - 1.5 Figures or illustrations to show all major configurations and identify all hazardous systems and subsystems
 2. Functional, power, and control circuit technical documentation and drawings (at a preliminary design level) reflecting known safety features, inhibits, controls, etc. Independence of inhibits and associated controls will be identified and documented.
 3. Provide preliminary drawings of components and mechanisms that show all major configurations, such as internal parts, flow paths, seals, housings, springs, position indicator switches, mechanical fluid fittings, electrical connectors, etc.
 4. Descriptions of safety-critical subsystems and their operations. For safety-critical software used to control a hazard or where loss of a safety-critical function or erroneous output can result in a critical or catastrophic hazard, provide (in addition to the hardware-related information above) an overview of the software architecture.
 5. Safety hazard analysis, HRs per Section 4.1.2, Hazard Reports, and appropriate supporting data per Section 4.1.3, Technical Data Supporting Hazard Analysis, including associated preliminary MHAs, Integrated Hazards, and common marginal hazards.
 6. Identification of non-compliances/variances.
 7. Description of CSMs and destination survival methods (captured as a list in HRs).

F.1.3.2 SUCCESS CRITERIA FOR A PHASE I SAFETY REVIEW

A Phase I review should be considered complete and successful when the CSRB concurs that the HRs are at a Phase I level. The CSRB will concur that the HRs are at a Phase I level when:

1. All hazard causes have been identified.
2. All identified preliminary controls for the hazard causes are acceptable as documented in the HRs and there is a direct link between the causes and their associated controls in the HR (signed by the HA Owner/Commercial Provider Project Manager).
3. The failure tolerance and hazard control approach being used is acceptable. FT exemptions with supporting rationale for DFMR are identified and concurrence is obtained from the CSRB. Hazard controls that must be provided by another Commercial Provider are clearly documented and identified, and agreement for the affected hardware has been obtained.
 - Identified and documented methods of survival for crew and Destination

- F-4
4. Software safety requirements have been identified, documented in the software requirements specifications, and analyzed for adequacy of control.
 5. Safety-critical subsystem and their operations have been identified, documented in the HRs.
 6. All AIs, with a Phase I closure timeframe, are closed and any remaining action/agreement items have been properly identified with assigned closure dates.

F.1.4 PHASE II SAFETY REVIEW

F.1.4.1 PHASE II DATA

The following list of Phase II data is formally submitted 30 days, or as negotiated with the Commercial Provider, prior to the safety review and should be made available as needed for delta reviews.

1. Updated SDP, HRs (signed by the HA Owner/Commercial Provider Project Manager), and appropriate support data.
 - a. A sufficiently detailed description of the approach that is planned to be used for each hazard control verification and why that approach will be suitable for verifying the intended function of that hazard control.
 - b. Updates to CSM and destination survival methods
 - c. Updates to MHA and IHA
2. Critical design details and concept of operations.
3. Updated design, build, and verification data (schematics, specifications, drawings, margins/safety factors, functional architecture, etc.) will be requested.
 - a. Updated interfaces, descriptions, schematics/figures, illustrations, and technical documentation and drawings reflecting detailed safety features, inhibits and associated controls, etc.
 - b. When shown in diagrams, the inhibits and their associated controls should be clearly labeled. Independence of inhibits and associated controls will be identified and documented.
4. For safety-critical software used to control a hazard or where loss of a safety-critical function or erroneous output can result in critical or catastrophic hazards, provide (in addition to the hardware-related information above) an updated overview of the software design, including state and mode diagrams. Also, provide an updated list of safety-critical software requirements applied to the design and a list of the hazardous commands and safety-critical computing system components.
5. Identification of non-compliances/variances.
6. Identification and documentation of all failures and anomaly history.

F-5 7. Status or closure rationales of open AIs and agreements assigned during the Phase I SRP review.

8. Documentation of newly identified hazards in existing or additional HRs

F.1.4.2 SUCCESS CRITERIA FOR A PHASE II SAFETY REVIEW

A Phase II review should be considered complete and successful when the CSRB concurs that the hazard reports are at Phase II level. The CSRB will concur that the hazard reports are at a Phase II level when:

1. Any additional hazard causes either through design changes or updated analysis have been identified.
2. All controls for the hazard causes, including controls related to exemptions, are acceptable as documented in the HRs and as implemented in the hardware or software design and there is a direct link between the causes and their associated controls in the HR. Independence of hazard controls should be confirmed (inclusive of updated list of CSM and destination survival methods).
3. All operational controls have been documented in a corresponding operational control database.
4. All verification methods for the hazard controls are acceptable as documented in the hazard reports.
5. Identification of non-compliances and evaluation of mitigations in HRs.
6. All AIs, with a Phase II closure timeframe, are closed and any remaining action/agreement items have been properly identified with assigned closure dates.
7. All critical failure modes are traced to their corresponding hazard cause(s).

All changes to the HRs from the previous safety review to the next should be marked using a method of tracked changes to aid in the review process. If the number of changes made is too significant, an updated HR may be submitted. If design changes warrant the deletion of a HR that was reviewed as part of the Phase I review, a brief statement of rationale for deleting the HR should be documented as part of the Phase II safety analysis.

All critical procedures/processes should be addressed, including the plan for verification. Include other safety material that is relevant. HRs should reference all applicable standards that will be used to comply with Program design requirements and verifications. Verification method **closure should be planned and identified for all hazard controls.**

F.1.5 PHASE III SAFETY REVIEW

F.1.5.1 PHASE III DATA

The following list of Phase III data is formally submitted 30 days, or as negotiated with the Commercial Provider, prior to the safety review and should be made available as needed for delta reviews.

- F-6
1. An updated safety hazard analysis, HRs (signed by the HA Owner/Commercial Provider Project Manager), and appropriate support data, including verification closure data or a closure plan.
 - a) Final list of CSMs and destination survival methods
 - b) Final MHA and IHA
 2. Finalized design, build, and verification data (schematics, specifications, drawings, margins/safety factors, functional architecture, etc.), including:
 - a) Final technical documentation, interfaces, descriptions, schematics, figures, illustrations, fabrication, assembly, testing, drawings reflecting detailed safety features, inhibits and associated controls, etc.
 - b) When shown in diagrams, the inhibits and their associated controls should be clearly labeled. Independence of inhibits and associated controls will be identified and documented. The schematics will reflect the as-built and as-verified design.
 3. For safety-critical software used to control a hazard or where loss of a safety-critical function or erroneous output can result in critical or catastrophic hazards, provide (in addition to the hardware-related information above) a final overview of the software design and a final list of the hazardous commands.
 4. Closure rationale of open AIs and agreements assigned during the Phase I and Phase II safety reviews.
 5. Resolution of non-compliances/variances
 6. Test reports and/or analyses concurred with by relevant SMEs
 7. For all hazard controls that cannot be verified as complete by the Phase III review, the Commercial Provider will provide and maintain a method of safety verification tracking as described in this section. The list of tracked verifications will be maintained by the Commercial Provider. Final formal approval of the HRs is considered complete when the final tracked safety verifications show that control verification has been successfully completed.

F.1.5.2 SUCCESS CRITERIA FOR A PHASE III SAFETY REVIEW

A Phase III review should be considered complete and successful when the CSRB concurs that all HRs are at a Phase III level of maturity. The CSRB will concur on the reports based on:

1. Any additional hazard causes either through design changes or updated analysis have been identified.
2. All controls for the hazard causes are acceptable as documented in the HRs and as implemented in the hardware design.

- F-7 3. All software safety requirements, safety-critical functions, and software controls have been tested to prove successful implementation and documented in the formal software test reports or a closure plan and ECD accepted by the CSRB.
4. All hazard control verifications have been completed or a closure plan and ECD accepted by the CSRB.
 5. All data used for acceptance rationale and justifications for the non-compliance/variance have been sufficiently identified and documented.
 6. All AIs, with a Phase III closure timeframe, are closed and any remaining action/agreement items have been properly identified with assigned closure dates.
 7. All required HR data fields are complete and accurate.
 8. All required contents of the SDP are complete and accurate, including identification of all applicable lessons learned as developed by the Commercial Provider.
 9. All Phase III HRs have been approved and signed by all appropriate boards.

Include any other safety material that is relevant. HRs should reference all applicable standards that will be used to comply with Program design requirements and verifications.

F.1.6 FLIGHT SAFETY CERTIFICATE DEVELOPMENT

A flight safety certificate or equivalent should document the following:

1. End item description (may capture multiple end items (part name/number) belonging to a single system on a single mission and transportation systems),
2. End item transport and stowage configuration, weight/dimensions, construction/materials (in addition, hazardous materials, non-standard metals, permanent magnets, cells/batteries, etc.),
3. End item's applicable transportation systems manifest or a currently on-orbit item requiring updated operations/stowage approval,
4. End item's safe design life and operational life, and
5. Formal safety endorsement for flight readiness.

F.1.7 VERIFICATION CLOSEOUT

Factors that drive schedule considerations are the following:

- Majority of the safety verifications are derived from hazard analysis, to demonstrate compliance with high level safety requirements, rather than specific system requirements.
- Some long lead analytical verifications are dependent on results from system tests and vice versa. Due to the linkage and duration of these verification activities successful completion frequently becomes a program milestone driver (critical path).

- F-8 • Limitations in ground testing may drive the need for analytical assessments to ensure safety margins are maintained in the flight environment.

F.1.8 BEST PRACTICES FOR SAFETY VERIFICATION TRACKING

A method of safety verification tracking is submitted as part of the Phase III SDP for each flight and should contain the following information at a minimum:

- a) Log Number
- b) HR Number/Title
- c) HR Cause/Control Number
- d) Verification Method with Status
- e) Description/Hardware (Control) Operation(s) Constrained
- f) Unique Associated Ground Operation Constraints
- g) Independent Verification Required? (Y/N)
- h) Scheduled and Actual Completion Date
- i) Method of Closure, Comments/Verification Completion Notice

F.1.9 SERIES, REFLOWN AND MODIFIED HARDWARE

For each series/reflow/modification hardware assessment, the following should be provided:

- a) Identification of all series/reflow/modification end items to be used and the baseline safety analyses by document number, title, and release date. If chemicals, biological materials, and/or ionizing radiation are used, provide a comprehensive listing, even if similar to those flown previously.
- b) Identification and assessment of changes in hardware/software and operations, provider roles which have safety impact.
- c) New or revised HR(s) with additional supporting data, and identification of HR(s) deleted or no longer applicable. Approved, baselined Phase III HR(s) should also be referenced.
- d) An assessment of the baseline safety verification methods to identify which verification(s) must be re-opened. This may encompass maintenance, structural inspections and/or refurbishment. Open verification items should be tracked under a method of safety verification tracking.
- e) Assessment of limited life items for series/reflow/modification end items, including a list which describes the failure mode and potential resulting hazard if they were to remain in service past their safe design and/or operational life.
- f) Assessment (including any corrective action taken) of all flight and ground failures and anomalies.

CLDP-STD-3102
Baseline - DRAFT

- F-9 g) Confirmation that the previously submitted flight certificate or equivalent remains valid for the updated transportation/operations scenario.

G-1 **APPENDIX G – BEST PRACTICES FOR SAFETY REVIEWS ROLES AND RESPONSIBILITIES**

G.1 END-TO-END MISSION PHASE

Each type of safety review has various roles and responsibilities for the Commercial Provider and NASA during E2E mission phases, and all operational phases, Table G.1-1, Mission Phase Safety Review Roles and Responsibilities outlines examples of the various types of safety reviews that might occur.

TABLE G.1-1 MISSION PHASE SAFETY REVIEW ROLES AND RESPONSIBILITIES

MISSION PHASE	SAFETY REVIEW	RESPONSIBLE PROGRAM
E2E	Crew Transportation System	Destination Provider-led with NASA Participation
	Cargo Transportation System	
	Integrated Destination/ Integrated Operations	
	Commercial LEO Destination (CLD)	
	Cargo (non-payloads)	
All Operational Mission Phases	NASA Sponsored Cargo (payloads only)	NASA-led with Destination Provider Participation
	Non-NASA Sponsored Cargo (payloads only)	Destination Provider-led with NASA Participation

G-2 G.2 CREW TRANSPORTATION SYSTEM SAFETY REVIEWS

In support of crew transportation system safety reviews between the Destination Provider and NASA, a full vehicle and system review (inclusive of integrated cargo) will be submitted by the CTS Provider. The review will focus on the launch and return phases, and will assess emergency response action (i.e., crew survivability/aborts) from an integrated system perspective including software, past flight/ground anomalies and any changes in design or operation. The Destination Provider will be responsible for monitoring and tracking all aspects of the mission until the USG crew arrives and integrated operations begin.

G.3 CARGO TRANSPORTATION SYSTEM SAFETY REVIEWS

In support of cargo transportation system safety reviews between the Destination Provider and NASA, a full vehicle and system review will be submitted by the CaTS Provider. The safety review will focus on the launch and return phases and will assess from an integrated system perspective including software, past flight/ground anomalies and any changes in design or operation. The Destination Provider will be responsible for monitoring and tracking all aspects of the mission until integrated operations begin.

G.4 INTEGRATED DESTINATION/INTEGRATED OPERATIONS SAFETY REVIEWS

In support of the integrated Destination system safety review, an integrated analysis will be submitted by the Destination Provider focusing on the integrated safety of the Destination and its crew for all operations within the Approach Ellipsoid. This analysis assesses the MWFs required to support USG crew and MNWFs that pose a risk to the USG crew, and identification and assessment of emergency response actions for both crew and destination survivability are also required.

G.5 CLD SAFETY REVIEWS

In support of the NASA and Destination Provider safety review, the Destination Provider is expected to submit an analysis focusing on Destination integrated with the launch vehicle. This analysis will evaluate the phase of the mission when the Destination is mated with the launch vehicle, as well as mission and ground system activities/operations related to launch and return. The Destination Provider will submit the HA for formal multi-board review.

G.6 CARGO SAFETY REVIEWS

Cargo safety reviews between NASA and the Destination Provider will support a review of Cargo, including ORUs, spares, logistical supplies, tools, crew preference items, payloads, payload facilities hardware (including impacts to the common environment, payload safety requirements, and systems, personnel, and equipment that is controlling the hazard (vehicle systems, procedures, etc.).

The HA is submitted by the Cargo Provider, and includes impacts to common environment and all systems, personnel, and equipment that is controlling the hazard.

G-3 The safety reviews are limited to Cargo and related activities the USG crew will interact with. The Cargo Providers will submit the HA for formal multi-board review.

Payloads have a unique case in which responsibilities vary based on who provides the payload and payload data.

NASA-led Cargo safety reviews are limited to payloads, and related activities the USG crew will interact with. Commercial Provider-led Cargo safety reviews are limited to non-NASA sponsored payloads, and related activities. The Cargo Providers will submit the HA for formal multi-board review.

G.7 COMMERCIAL PROVIDER SAFETY BOARD PROCESS BEST PRACTICES

The Commercial Providers should be responsible for the following tasks to demonstrate compliance to the safety process:

- Maintain Safety Board process information and other related material under a formal configuration management process,
- Implement real-time status and associated processes,
- Maintain a master schedule for end item and integrated safety reviews,
- Lead safety reviews as established in processes and infrastructure,
- Record, track, and resolve assigned safety board actions,
- Record and retain for archive minutes of safety reviews, WGs, and outside of board meetings,
- Incorporate new safety findings, technologies, and methodologies on a regular basis into safety analysis/supporting data,
- Engage a wider range of stakeholders in the review and improvement process to gather diverse perspectives and expertise,
- Provide technical and management resources necessary to ensure the overall safety and protection of flight and ground personnel, general public, flight/ground hardware, the environment, transportation systems and facilities through all phases of the applicable contract, including oversight of subcontracted efforts,
- Provide NASA access to the prime Commercial Provider's and Commercial Provider Subcontractor's safety data,

- G-4
- Develop training modules or guidelines to help users understand and effectively apply the document's requirements and recommendations, and
 - Comply with launch site safety requirements, and ground safety requirements. Appendix K, Best Practices for Ground Safety, provides additional guidance and best practices for ground safety processes.

G.8 SAFETY REVIEW COMPLETION

Successful completion of Phase III reviews is normally accomplished by obtaining approval of all HRs containing critical and catastrophic hazards.

The Commercial Provider should meet the following criteria for successful completion of a Phase III safety review:

- Safety review AIs/agreements associated with HRs are formally closed, if applicable.
- Final updates to non-compliance/variance rationale incorporated in HRs, if applicable.
- Board comments have been dispositioned. HA Owner/Commercial Provider disposition of comments are discussed at the phased safety review.
- If all activities associated with the safety review (other than open verifications) are completed, all HRs are signed by the Commercial Provider Board delegated authority, and NASA Chairs at the Phase III level.
- Final list of tracked safety verifications referenced in Section 4.2.7, Safety Verification Tracking.
- Final signed SDP submitted by HA Owner/Commercial Provider Project Manager or delegated authority after successful completion of the items above. Final safety assessment approval by NASA, when applicable.
- Final signed Flight Safety Certificate, or equivalent, referenced in Section 4.2.5, Flight Safety Certificate.

G.8.1 HR DISPOSITION

Applicable safety products and HRs will be formally dispositioned upon conclusion of each phased safety review. This includes the Safety HA, SDP, and HRs. Concurrence from the Commercial Provider Program Manager or Delegated Authority is required to close out these products.

This disposition will be one of the following:

- Approved,
- Approved with Modifications:

Concur with an action/agreement/modification to be performed by the HA owner/responsible organization. HA Owner/Commercial Provider completes edits during or following the safety review.

CLDP-STD-3102
Baseline - DRAFT

- G-5 • Deferred:
- Consensus was not reached for HR approval. Further technical discussions necessary prior to board approval of HR.
- Withdrawn:
- HR/HR Cause is superseded or deleted.

H-1 APPENDIX H – GOVERNMENT FURNISHED SERVICES TRANSPORTATION

H.1 GOVERNMENT FURNISHED SERVICES

NASA will initially offer Government Furnished Services (GFS) Transportation **<TBR H-1>** and leverage heritage CTS and CaTS as a GFS that the Commercial Provider may utilize during the initial operations of the CLDS. To certify usage of these systems, a delta phase safety review is required to validate that the present configuration satisfies requirements and baselined hazard assessments.

A delta phased safety review is completed by the Commercial Provider and NASA by performing the following:

- a) Leverage existing design
- b) Re-evaluate hazard assessments/gap assessment
- c) Assess for new hardware, software upgrades, ops con changes, etc.
- d) Assess for potential increase in risk
- e) Ensure all modifications do not invalidate baseline/approved HRs
- f) If the gap assessment discovers significant design, software or operational changes, a phased safety review will be required as outlined in Section 4.2, Safety Milestones.

NASA plans to transition responsibility for these transportation services to the Commercial Provider. NASA and Commercial Provider roles and responsibilities will be defined and documented in separate agreements for both the GFS Transportation agreement period and the E2E services portion of the joint agreements.

I-1

APPENDIX I – IMPORTANT NASA/NESC MEMOS

HR templates contain references to additional safety policy memos and/or technical requirement interpretation letters to aid the Commercial Providers in documenting hazard controls/verifications. Table I.1-1 lists the referenced documents. Forms serve as an aid to providing the required data for safety review. Figure I.1-1, Battery Description Form, provides an example of an available form. Referenced documents and forms can be found in the technical library and made available upon request.

**TABLE I.1-1 POLICY MEMOS/TECHNICAL REQUIREMENTS INTERPRETATION LETTERS
(2 PAGES)**

Document Number	Document Title
EC-22-089	“Predicting On-Orbit Surface Temperatures of Powered Devices Using Analysis,” attached to IHS Record 64309
EC-22-091	“Use of Thin Coatings to Mitigate Touch Temperature Concerns,” attached to IHS Record 64309
EP-18-113	Safety Requirements for the use of Electrolytic Capacitors in ISS End Items
ES4-22-030*	Toxic Offgassing Exemptions
JWI 8705.3	Battery Processing for Crewed Space Vehicle Applications
NASA-HDBK-5010	Fracture Control Implementation Handbook for Payloads, Experiments, and Similar Hardware
MA2-00-038	Interpretation of On-Orbit Maintenance
DA9-05-029	On-Orbit International Space Station Systems Maintenance
MA2-99-142	On-Orbit Bonding and Grounding
MA2-99-170	Crew Mating/Demating of Powered Connectors (Interpretation for Inhibits)
TOX-VR-2021-03*	Evaluation of Particles/Dusts in Habitable Spacecraft
NESC-IB-24-01986	Failure-Tolerant Avionics for Crewed Space Systems Recommended Best Practices
ES4-24-030	Flammability Memo
NESC Technical Bulletin 24-05	Safety Critical Avionics TM-20240009366
NESC TB 22-08	High Purity Hydrazine Contaminants
AFRL-RZ-ED-TP-2008-184	Nitrous Oxide Hazards
AIAA SP-086-2001	Fire, Explosion, Compatibility, and Safety Hazards of Nitrogen Tetroxide (NTO)
AIAA SP-085-1999	Hazards of Hypergols MMH
NASA TB 19-02	Double Wall Radiography of Metallic Pressure Vessels
NASA NESC TB No.20-07	Bond Line Sensitivity for Prop Tanks
AIAA-G-082	2022 Guide: Space Systems – Composite Overwrapped Pressure Vessels with a Plastic Liner
NESC TB 22-07	Prop Feed Dissolved Gases Come out of Solution Thru Pressure Drops
NESC TB 22-02	Prop Filter Design
NESC-RP-19-01498	Filtration of Spaceflight Prop and Pressurant Systems
JANNAF-GL-2022-0001	Guidelines for Combustion Stability Specs and Verification Procedures

I-1

CLDP-STD-3102

Baseline - DRAFT

I-2

Document Number	Document Title
NASA TM-20210022275	Treatment of Transient Pressure Events in Space Flight Pressurized Systems
TOX-VR-2023-01*	Evaluation of Particles/Dusts in Habitable Spacecraft
TOX-VR-2022-05*	Toxicological Assessment of Aldehyde Vapors in Spacecraft
TOX-VR-2023-04*	Evaluation of Simple Asphyxiant Gases in Habitable Spacecraft
TOX-VM-2014-07*	Offgas test (OGT) requirements for closed-loop spacesuits
TOX-VR-2024-02*	Ingress precautions based on toxicity hazard index (T value)
TOX-VR-2023-02*	Toxicological Assessment of Liquid Crystal Displays
TOX-VR-2017-01*	Evaluation of LiOH in Habitable Spacecraft
TOX-VR-2022-02*	Toxicological Assessment of Elemental Mercury (Hg) Sources in Spacecraft

* The latest revision of the document should be used

Forms serve as an aid to providing the required data for safety review. Excerpts of the forms are below:

For the Phase 0/I Safety Data Package, provide the following information:

1a. Hardware Point-of-Contact:
(Name/Company/Phone/Fax/email)
TBD

1b. Hardware Name: TBD

Hardware Part Number: TBD

Hardware Acronym: TBD

Battery Name: TBD

2a. Hardware / Battery Managing Group, Company, or Agency:
TBD

2b. Hardware and Battery Environmental Requirements:
Thermal Environment (max, min, operational and non-operational ranges):
TBD
Pressure Environment (EVA, IVA):
TBD
Life (calendar/shelf, cycle/service):
TBD

3a. Battery and Hardware Description:
Is the battery pack (including all components) Commercial-off-the-shelf (COTS)? ☐ Yes ☐ No
Function/Operating modes (continuous, pulse, intermittent, clock backup, memory, etc.):
TBD
Battery/Cell crew access on-orbit? ☐ Yes ☐ No
Short Description of Battery System: (Number of batteries to be flown; details if multiple batteries are required to power Application, unique design information, etc.)
TBD

3b. Cell Description:
Chemistry (If Li-ion, what type: NMC, NCA, FePO4, etc.): TBD
Cell size: TBD
Manufacture and Model: TBD
Nominal OCV: TBD Maximum Voltage: TBD Minimum Voltage: TBD
Rated Capacity: TBD
Maximum Rated OEM Discharge Current: TBD
Maximum Recommended OEM Charge Current: TBD
Minimum and Maximum OEM Discharge Temperatures: TBD
Minimum and Maximum OEM Charge Temperatures: TBD
Minimum and Maximum Storage Temperatures: TBD
Date of Manufacture (Mo/Yr): TBD

3c. Battery Information: (9 V COTS batteries shall be considered as single unit)
Quantity of total cells: TBD
Cell connectivity (IPAS, #SAP): TBD
Operational Battery Environment Temperatures Range (Min/Max): TBD
Nominal OCV: TBD Maximum Voltage: TBD Minimum Voltage: TBD

For the Phase II/III Safety Data Package, provide the following information:

Storage location (launch and on-orbit use locations):
TBD
Packaging and hardware approved by flammability group (reference requirement):
TBD
Is the battery charged on orbit?, Yes: ☐ No: ☐
If yes, describe charge rate, charger hardware, and protections to prevent overcharge
TBD
Is the battery being discharged on-orbit? Yes: ☐ No: ☐ If yes what is the discharge rate(s):
TBD
Circuit Description and Electrical Schematic (attach electronically or reference location in HR):
TBD
Summary of circuit protections and include trip/reset points (i.e. fuses, diodes, MOSFETs, resistors, source isolation, etc.):
TBD
Battery testing complete and report uploaded to this HR? Yes: ☐ No: ☐
If yes, provide a short summary test results including anomalies or failures.
TBD
Has the pre-flight processing, flight acceptance plan, on-orbit processes, operational constraints, and the on-orbit and post-flight battery disposal plan for the hardware been conducted in accordance with JWI 8705.3?
Yes: ☐ No: ☐ If yes, provide accompanying documentation.
TBD

End of document

FIGURE I.1-1 BATTERY DESCRIPTION FORM

I-2

This document has been approved for public release per STI 20250008716.

APPENDIX J – COMMENTS DOCUMENTATION

J-1

J.1 COMMENTS

Comments are a way to track and document technical questions, changes, and concerns from the safety community. During the review period, comments will be given to the Commercial Provider by members of the CSRB. The comments provided by the CSRB will cover hazards, control, causes, verifications, and/or supporting documentations, etc. The Commercial Provider should respond to the comments and work towards a resolution of closing the comments.

Commercial Providers should specify the communication method they prefer to utilize for comment exchange. The following sections covers different ways to document comments.

J.1.1 COMMENT SHEET

The use of a comment sheet is a way to document the hazard categories (hazard, control, cause, verification or supporting document comments). The comments would be listed per hazard category and/or where the comment is referenced in the SDP, HRs, or supporting document. This comment sheet tracks the written discussions between the commenter and the Commercial Provider. The comment sheet will be distributed, compiled, and regulated by a member of the CSRB.

The advantage of the comment sheet is that all the comments are documented in one place. Therefore, it will be harder for the Commercial Provider to miss a comment and not respond to all comments.

The comment sheet may be uploaded and maintained in a predetermined database for ease of tracking/management by all stakeholders.

Comment Form					
System/Payload Name:					
Phase/Type of Review:					
Safety Panel Engineer (SPE):					
Hazard Category (choose from drop down menu)	IHS Record #	Comment Location (Record Title/File Name, Cause/Control/Verification Number and Title, etc.)	Assessment and Recommendation	Commenter Name/Discipline/Program Org	Response from Provider

Evaluator	Document #	Section/Para #	Comment Type	Comments	Dispositions

FIGURE J.1.1-1 EXAMPLES OF COMMENT FORM

J-2J.1.2 REDLINES

The use of redlines is a way to document the comments at the exact point of reference. The comments should be attached to a phrase, sentence, or word of the section it is applicable to. The Commercial Provider should be able to reply to the commentator directly on the comment.

The advantage to redlines is that it creates an easier method of communication between the commentator and the Commercial Provider.

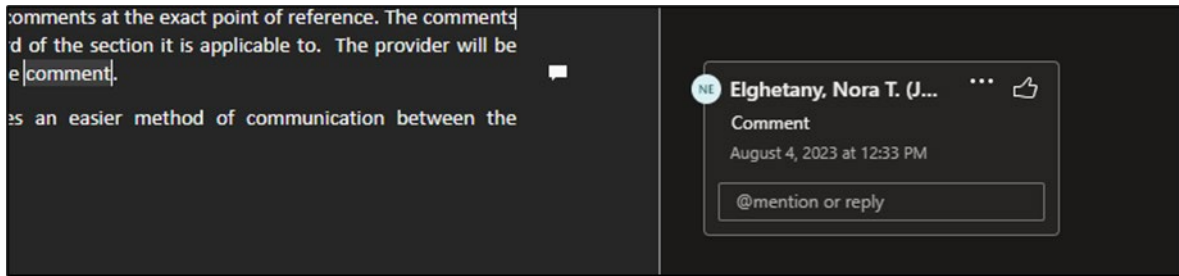


FIGURE J.1.2-1 COMMENTS EXAMPLE

K-1 **APPENDIX K – BEST PRACTICES FOR GROUND SAFETY**

The following section describes best practices for the ISSP ground safety process. This section serves as guidance for payloads being processed at Kennedy Space Center (KSC), Wallops, and other launch sites and is intended solely as an example for Commercial Providers **<TBR K-1>**. Facility processing at NASA sites described herein may not precisely reflect actual procedures and prioritization at those facilities and processes may differ for CLDP.

K.1 **GROUND PROCESSING AT KSC**

The Ground Safety Review Panel (GSRP) is responsible for assuring ground safety for hardware being processed, tested, and/or operated at KSC in accordance with the requirements in KNPR 8715.3, KSC Safety Procedural Requirements. Safety data submittal for the ground safety review process (conducted by the GSRP) is required only at the Phase III level; Phase 0, I, and II reviews are not required. Following successful completion of the ground safety review, the GSRP will issue a letter of approval for processing at KSC. The letter of approval will note any open safety verifications and list associated constraints. Payload developers are encouraged to contact the GSRP to discuss any questions or issues regarding payload design, GSE design, ground processing operations, or documentation submittals.

Payload developers will submit the KSC Form 50-341, Ground Safety Checklist and all associated documentation to the GSRP no later than 30 days before the start of processing operations at KSC. The form and submittal instructions can be found on the GSRP website:

<https://nasa.sharepoint.com/sites/GSRP/>

The Ground Safety Checklist submitted to the GSRP will include:

1. Administrative Data
 - a. Payload/Hardware Owner – Payload point of contact and their organization
 - b. Payload/Hardware Name
 - c. Flight/Mission
 - d. KSC Arrival Date
 - e. KSC Departure Date
 - f. KSC Processing Location (e.g., Space Station Processing Facility (SSPF) High Bay Footprint, Offline Laboratory, etc.)
2. Description of Payload and Ground Operations – Provide a summary of ground operations, detailing planned events including major processes, locations, and hardware involved (including post-flight operations being carried out at KSC). Include a picture or rendered image of the payload and an approximation of the payload mass. Describe payload subsystems and safety features/inhibits.

- K-2³. Hazardous Operations – Provide a list of hazardous operations to be performed. Document the hazard controls in HRs. Verifications that are incomplete at the time of submittal will be listed using a method safety verification tracking and tracked to closure. Include the tracked safety verifications in the submittal to the GSRP. Any Non-compliances/Variations with safety requirements will be clearly identified and documented in the relevant ground HR.
4. Chemicals – Provide a list of hazardous chemicals or materials to be used for processing at KSC. Provide the chemical manufacturer Safety Data Sheet for each hazardous chemical/material.
 5. Biological Hazards – Provide a hazardous material summary list/table for each hazardous biological substance to be used for processing at KSC. Note: The hazardous material summary list/table is a flight product, but the GSRP uses it as a reference to enhance its understanding of certain materials.
 6. Ground Pressure Systems – Summarize ground system pressure operations to be performed at KSC. Pressure systems will be compliant with Industry Standards and designed and used for their intended purpose.
 7. Flight Pressure Systems – Summarize flight system (e.g., Composite Overwrapped Pressure Vessel (COPV), Constant Pressure Valve (CPV)) pressure operations to be performed at KSC. Pressure systems will be compliant with Industry Standards and designed and used for their intended purpose.
 8. Explosive Commodities – Summarize (type, quantity, usage, location) any explosives, propellant, or pyrotechnics being brought to KSC (the GSRP will provide this information to the KSC Explosive Safety Officer).
 9. Ground Support Equipment – Identify any ground support equipment being brought to KSC (e.g., lifting devices; spreaders, beams, slings). Ground support equipment will be compliant with Industry Standards and designed and used for its intended purpose.
 10. Radiation – Identify any ionizing (e.g., radioactive material, ionizing radiation producing equipment) or non-ionizing radiation sources (e.g., laser, radio frequency (RF) radiation 3 kilohertz (kHz) to 300 GHz, sunlight radiation, and artificial incoherent light sources).
 11. Batteries – Identify non-alkaline batteries (e.g., Lithium Polymer (Battery) (LiPO), Lithium Plus Ion (Li-Ion), Nickel Hydrogen (NiH₂) to be stored, charged, or discharged at KSC. Summarize operations involving batteries.
 12. Films, Foams, and Tapes – Identify plastic films, foams, and adhesive tapes used during ground processing. Provide data sheets and any available test data for materials not listed in KTI-5212. KTI-5212 is available on the GSRP website.
 13. Hot Work – Identify all planned hot work, such as soldering, welding, brazing, casting, forging, injection molding, laser cutting, plasma cutting, additive

K-3 manufacturing, baking, microwaving, autoclaving, thermal vacuum testing, use of electrical arcs, open flames, etc.

14. Software – Identify software that controls a hazard and/or software that can initiate a hazard during ground processing.

The GSRP may request the following items in addition to the data required in the Ground Safety Checklist:

1. Ground operations procedures.
2. Engineering drawings and stress analyses of safety critical subsystems.
3. Proof-loading evidence.
4. Pressure Vessel and Pressurized Systems certifications.
5. A summary of safety-related failures and accidents involving flight hardware or GSE.
6. Verification that each flight system pressure vessel has a pressure vessel logbook showing pressurization, history, fluid exposure, and other applicable data.

NOTE: Radiation sources must receive a separate evaluation from the KSC Radiation Protection Committee (RPC)—see Radiation Use Authorization on the GSRP website. Payload developers will notify the GSRP of all radiation sources no later than 90 days before the start of processing operations at KSC. The GSRP will liaise with the RPC to determine the appropriate documentation for each payload developer, as the required documentation varies by type of radiation source. Payload developers will submit the agreed-upon radiation documentation to the GSRP no later than 60 days before the start of processing operations at KSC. The GSRP will provide the payload developer's radiation documentation to the RPC for review. Approval from the RPC is a constraint to operations involving radiation sources and will generally be treated as a constraint to final approval from the GSRP.

After the GSRP has issued a letter of approval, payload developers will provide an updated safety assessment to the GSRP if there are changes to the payload design, GSE design, ground processing operations, or ground hazards.

K.2 GROUND PROCESSING AT KSC FOR SERIES/REFLIGHT HARDWARE

For series/reflights with no new hazards, no increase in safety risk, no changes to payload or GSE design, and no new processes, the payload developer is not required to submit a new Ground Safety Checklist. For situations where it is unclear whether or not a new Ground Safety Checklist is required, contact the GSRP for a determination. Payload developers who are not required to submit a new Ground Safety Checklist will notify the GSRP of the expected processing dates. The GSRP will issue an approval letter for series/reflights.

K-4 K.3 TRANSPORT VEHICLE GROUND SAFETY
K.3.1 USCV AND CRS LAUNCH SITES

For hardware transported on a United States Crew Vehicle (USCV) or Commercial Resupply Services (CRS) transport vehicle, ground safety reviews are conducted between the USCV or CRS Provider and the range in accordance with USCV/CRS requirements. Hardware ground safety input data will be captured via completion of Destination hardware data sets (cargo integration data) as documented in SSP 50835, SSP 57000, SSP 57003 or the applicable unique hardware to transportation system ICD/IRD/Interface Requirements Baseline (IRB). Additional hardware ground safety data may be requested to support USCV or CRS provider development of ground SDPs and plans.

K.3.2 NASA WALLOPS FLIGHT FACILITY

Hardware delivered, processed, tested, or operated at NASA GSFC Wallops Flight Facility (WFF) that are considered hazardous activities to WFF personnel and facilities and then stored as cargo will be evaluated and are approved by GSFC WFF Safety and Mission Assurance in accordance with GSFC/WFF Range Safety Manual, NASA GSFC-STD-8009, and other applicable governing requirements listed within this manual. These hardware items include, but are not limited to, pressurization of flight or ground pressure vessels, fueling operations of flight payloads, RF transmitters, lasers, ionizing radiation sources and/or many other activities that are considered hazardous operations. Hardware delivered and processed, but not tested or operated, and not considered hazardous at WFF, but require WFF SMA review or evaluation.

L-1

APPENDIX L – DFMR CONTROL APPROACH GUIDANCE

The following section outlines the DFMR control approach utilized by other programs and may be used as additional guidance. For the ISS program, DFMR is an alternate approach to FT using the safety related properties and characteristics of the design to reduce the associated risk to an acceptable level. Hazards related to DFMR are controlled by the safety-related properties and characteristics of the design, such as margin or Factors of Safety that have been baselined by ISSP requirements.

The information provided in Appendix L is intended to be used as historical examples of use of DFMR from other programs. The “shall” statements contained in this Appendix section are historical statements from other programs and are non-enforceable to CLDP. References and requirements used by other programs may not contain applicable standards in the CLDP program. Any similar DFMR proposals for CLDP should reference CLDP applicable requirements and standards.

New DFMR candidates will be coordinated, reviewed, and approved as part of the Safety Data Package.

Table L.1-1 provides the DFMR Control Approach utilized by the ISS program:

TABLE L.1-1: ISS EXAMPLE DFMR LIST (4 PAGES)

DFMR End Item	DFMR Approach
Liquid Electrolytes/Caps	1. Preliminary structural verification plan.
Cooper Separation Nuts	1. Compliant with the qualified capabilities, specifically: ○ Thermal and loads environments ○ Fracture control Methodology
Galling Jamming Fasteners	1. One layer of fault tolerance via rigorous design, analysis and testing rather than through true physical redundancy
	2. Most of the requirements which apply to threaded interfaces have to do with addressing
	3. Type of thread. Certain types of threads by design have a higher probability of galling/jamming than others.
	4. Lubrication
	5. Protection during flight
	6. Thermal analysis and testing

L-1

L-2

DFMR End Item	DFMR Approach
Quick Release Pins	1. Mechanisms, meet requirements of MA2-00-057
	2. Qualification vibration test
	3. Environment acceptance test
Battery	1. Thermal runaway propagation is generally covered under the internal short section as DFMR and is in the HR template
Bonding/Grounding	1. MA2-99-142 This letter defines criteria for satisfying bonding and grounding requirements when hardware installation occurs on orbit. Two acceptable methods are the preferred DFMR approach and the alternative Failure Tolerance approach. These criteria apply when crew contact with voltages above 32 volts (root mean square or direct current) is possible following normal procedures or after potential electrical or mechanical failures. In both cases, a fault bond path shall be established before power is applied.
Springs	1. Redundant
	2. Or designed, evaluated, and used in NASA-STD-5003
Fasteners Retention	1. Positive locking (locking inserts, locking threads)
	2. Not using locking compounds when other locking devices are practicable
Strength and Fracture Control	1. Designed with sufficient strength to tolerate actuation force/torque stall
	2. Included in an acceptable fracture control plan
	3. Where applicable, mechanical stops designed to worst case dynamic loading conditions
	4. Design to remote manipulator systems and EVA, IVA impact loads
	5. Must preclude deformation that could cause binding/jamming/seizing or inadvertent actuation

L-2

L-3

DFMR End Item	DFMR Approach
	6. Comply with NSTS 08307 preload criteria
Positive Indication of Status for Safety Critical Mechanical Systems	1. Provide positive indication mechanism is in desired position
	2. Have end of travel stops
Torque/Force Margins	1. Be acceptance test verified
	2. Submit to Mechanical Systems Working Group (MSWG) for review and approval for other margin verification methods (analytical/ combo of analytical and testing)
	3. Margin verification, test, analytical account for worst case
	4. Be acceptance test verified
Contamination of Safety Critical Mechanical Systems	1. Be fabricated and handled in a clean environment to avoid chemical and particulate contamination
	2. Have specific cleanliness requirements established/stated
Assembly Level Acceptance Test For Qualification and Flight Safety Critical Mechanical Systems Assemblies	1. Undergo run-in testing
	2. Undergo function and environment acceptance testing
Qualification Tests for Safety Critical Mechanism Systems Assemblies	1. Establish a qualification test program, which shall assure design performance and safety margin exists with respect to all requirements
Design Life Verification Tests	1. For endurance, fatigue, lubrication deterioration, and/or excessive wear are a concern, design life verification testing
	2. Be conducted to establish design life requirements are met
Sealing Surfaces, Bladder Tanks	
DFMR Designation by MSWG is For Movable Mechanical Systems Only	1. Single level of control
	2. Failure of primary structure, structural failure of pressure vessel walls, failure of pressurized lines

L-3

L-4

DFMR End Item	DFMR Approach
	are excepted from failure tolerance requirement provided the potentially catastrophic failures are controlled through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance
Structures, Pressure Vessels, Pressurized Lines, Functional Pyrotechnic Devices, Mechanisms in Critical Applications, Material Compatibility, Flammability	1. Hazard controls related to these areas are extremely critical and verification of compliance on the part of the payload organization and the visiting launch vehicles
PIP Pins	1. PIP Pins approved as a DFMR mechanism
NASA Docking System (NDS)	1. (D683-102100) NDSB1 Safety Assessment Report
	2. DFMR Mechanisms

ISS DFMR approach for the failures of Mechanisms, Moving Mechanical Assemblies (MMAs), or Mechanical actuators in the Binding/Jamming/Seizing failure mode are excepted from the failure tolerance requirement, provided it can be shown that they have been designed to meet the intent of all applicable requirements in NASA-STD-5017B, and a Hazard Analysis has been completed in order to: 1) recognize the importance of the hazard being controlled, 2) ensure robustness of the design, and 3) ensure adequate attention/focus is being applied to the design, manufacture, implementation, testing, analysis, and inspection of the mechanism. Whenever a mechanism can practically be designed to use redundancy (failure tolerance) to protect for catastrophic hazards, it shall be. However, it is often not possible or practical to implement Failure Tolerance in some Mechanisms or Mechanical systems for the mechanical Binding, Jamming, or Seizing failure mode. While it is possible to include redundant protection measures for certain rotating joints or surfaces, many types of devices are susceptible to jamming because a redundant solution cannot be provided due to the inherent nature of their design function. (A few examples include thrust vector control actuators, aerosurface position actuators, landing gear oleo struts, landing gear extend actuators, pneumatic piston actuators, gear trains or gear boxes, certain valve types, and certain mechanical dampers, among others). In such cases, attempting to provide mechanical redundancy would add detrimental mass, volume, power draw, and/or complexity to the system, and potentially introduce new failure modes, some of which may not be readily apparent. As such, attempting to introduce mechanical redundancy in these devices may reduce overall system reliability rather than increase it. For these special circumstances, adding Failure Tolerance is NOT the most appropriate method of controlling the critical hazard of mechanical binding, jamming, or

L-5 seizing. Therefore, the overall goal of mechanical safety and reliability for inherently zero-fault tolerant mechanisms shall be achieved by meeting the intent of all applicable requirements in NASA-STD-5017B, both for the design and for testing, and by completing a thorough hazard analysis.

For the Gateway program, Exemption A is the equivalent to DFMR and considered an exemption to Failure Tolerance without the need for an NCR. Exemption A items are typically controlled either via standards and margins, or via standards and compatibility with worst case environments. In all cases, system designs must demonstrate that they meet or exceed the intent of a defined process in which NASA- or Gateway-approved standards and margins are implemented with the use of worst-case conditions.

Following are DFMR approach examples utilized by the Gateway program:

- Micro-Meteoroid Orbital Debris strike results in immediate catastrophic effect
- Hardware susceptibility to total dose effect of radiation
- Primary Structures
- Welded Interfaces
- Metallic seals
- Mechanisms that are fully engaged and providing a structural function
- Wire derating
- EMI hazards
- Flammability controlled by material compatibility
- Toxic exposure hazards controlled by material off-gassing compatibility (applies to air and water).
- Sharp edges
- Leakage of tubing
- Entrapment
- Susceptibility to lasers
- Batteries – part of JSC 20793 require compliance with standards
- Pyro susceptibility to environment
- Acoustics
- Touch Temperature
- Shatterable/Brittle Materials

For the Orion program, the following excerpts are taken from MPCV-70038 Rev B:

MPCV-70038 Rev B, Section 3.2.3, Design for Minimum Risk (DFMR)

DFMR is a method used to design a system so that it will continue to safely operate even when exposed to highly variable conditions. The hazards of the system are controlled through a defined process in which approved standards and margins are implemented to account for the inability to implement FT. This method minimizes the

L-6 likelihood of occurrence of a hazardous effect by increasing design margin in the system based on the capability of the material, the operating environment, and their known variability. Application of margin may be implemented through increased dispersion of the environment or system properties that respond to the environment. The use of DFMR shall be declared and meet the DFMR approval process per Section 3.2.2.1.

Implementation of DFMR is an option for failure of primary structure; structural failure of pressure vessel walls; structural failure of pressurized lines and welded joints; and the Thermal Protection System (TPS) tiles and ablator. Structural failure of pressure vessels or pressurized lines is interpreted as failure due to rupture, collapse, or excessive deformation, resulting in the inability of a structure to sustain specified loads, pressures, and environments (except for micrometeoroid and orbital debris (MMOD)). Other failure modes associated with pressurized lines such as blockage due to freezing or contamination, over-pressurization due to system failures (e.g. pressure regulators, sensors, or valves), leakage through seals or non-welded interconnections, or failure or degradation due to MMOD, should not be interpreted as DFMR.

MPCV-70038 Rev B, Section 3.2.4, DFMR Approval Process

DFMR candidates are not automatically exempted from failure tolerance. The Program Manager (or delegate), Technical Authorities, and Flight Crew must all concur that the appropriate design standards and other controls are in place to reduce the risk of hazard occurrence to an acceptable level. The process by which this assessment is performed and approved is specified by this document. If the Program Manager, Technical Authorities, or Flight Crew cannot agree with the proposed controls or the residual risk, then the system designer may be directed by the Program Manager to make changes to reduce the risk. Adequate rationale for the acceptance of residual safety risk, when submitted, may require the need for controls above and beyond the standard program requirements. In addition, the NASA community may require additional controls prior to approving.

Candidates for DFMR shall be identified early in the Concept Development phase through the Preliminary Design phase and documented in the PHA. The PHA and resulting Hazard Reports (HR) are delivered as part of the Preliminary Design Review (PDR) Safety Data Package (SDP) and reviewed during the Phase I Safety Review.

The MPCV Safety and Engineering Review Panel (MSERP) (including Technical Authorities) will review and concur on the approach for controlling flight hazards, including candidates for DFMR and OFT applications, prior to completion of the Phase I Safety Review. Criteria for acceptance of DFMR or OFT as a design solution shall include at a minimum, control of the hazard through a defined process in which approved standards and margins are implemented that account for the absence of failure tolerance as well as a record of historical data indicating successful implementation of the specific control strategy.

Use of DFMR as a hazard control will be briefed at project milestone reviews. The MPCV technical panels and WGs will support the process as required by:

CLDP-STD-3102
Baseline - DRAFT

- L-7 a) Assisting in the development of acceptable control strategy for DFMR items
- b) Providing assurance that all credible hazards and failure scenarios have been identified and are reliably and effectively controlled as a result of a through design, build and test process.
- c) Ensuring that appropriate verifications are in place and satisfied for the chosen DFMR control strategy

M-1 APPENDIX M – BEST PRACTICE EXPECTATIONS – NASA SEVEN ELEMENTS OF FLIGHT RATIONALE

For the STS-114 Return to Flight Activity, Engineering developed seven steps, which were baselined in the Shuttle Program, as the way to approve technical issues for flight. These Seven Elements of Flight Rationale are defined as questions to be answered whenever there is an issue related to unexpected behavior of a system/subsystem/component outside of design intent in lieu of just accepting “in family” as adequate rationale. Each of these elements need discussion and can be scored by the evaluator in relation to risk posture definition, with mitigation options, to be communicated to the Program/Agency for consideration.

NASA engineering will expect the provider to use the following expectations format on disposition of technical issues pertaining to human spaceflight safety.

Seven Elements of Flight Rationale

1. Solid technical understanding
 - a. Why are we making this change? What problem are we addressing? Do we know what we are giving up? How well do we understand the fix? Are the critical features inspectable? Is the process under control?
 - b. Do we know how/why this condition occurred (impact, scrape, age out, moisture loss, residual stress, etc.)? Do we understand root cause? Did we use a fault tree? Do we understand the extent of the crack, high-density indication (HDI), damage, foreign object debris (FOD), etc.? Do we know what the foreign material is? What are the plausible contaminants and how could they be harmful?
 - c. Do we understand how/why components with similar indications performed the way they did? Is there a fix/repair for this unit/article? Do we understand the repair process/condition? Are the generic design and process robust and in control?
2. Condition relative to experience base
 - a. Have we dealt with this problem before? How is this the same? Different? Do we have flight or test history with this defect? With this repair? Other motors or programs? How are we the same? Different? Was the similar feature actually exercised in a test? What was the outcome?
3. Bounding case established
 - a. What bounding scenarios (test, analysis, etc.) have been evaluated in the attempt to bound or envelope the issue (e.g. upper 3 σ loads, lower A basis allowables, a specific worse hardware condition)?

- M-2 b. What assumptions were made? Where are they conservative? Not? Were all the failure modes addressed? Have we considered the “what if we’re wrong” scenarios?

4. Self-limiting aspects

- a. Physical reasons why the defect or condition will not get worse than current state or degrade. Why can the condition never exceed the bounding case?
- b. Is the system fail safe or fault/failure tolerant? Are there built-in redundancies if the feature does fail? Are all the critical features/operations inspectable?

5. Margins understood

- a. What are the predicted margins for the discrepant or repaired part? Have they changed from baseline? What are the margins for the bounding case?
- b. Is the component/feature in an area of high or low thermal or structural margin? How far are we from a cliff?

6. Assessment based on data, testing and analysis

- a. Is the final assessment based on test data and analysis or on expert opinion and gut feel? Where do we actually have data? Where are we guessing? Was the test/measurement/analysis technique standard and proven or new?
- b. Do we understand all the assumptions that went into the assessment? Does the analysis/assessment rely on a series of dependent assumptions (where an error could propagate) or are there independent elements or blocks?

7. Interactions with other elements/conditions addressed

- a. Are there any known, compounding interactions with other issues, components, changes, etc.? How have the potential interactions been identified? How/when will they be addressed?