National Aeronautics and
Space Administration

ESD 10010
REVISION B
RELEASE DATE: 03/03/2016

EXPLORATION SYSTEMS DEVELOPMENT SAFETY AND MISSION ASSURANCE PLAN

Publicly Available: Release to Public Websites Requires Approval of Chief, Office of Primary Responsibility

The electronic version is the official approved document.

Verify this is the correct version before use.

REVISION AND HISTORY PAGE

Revision No.	Change No.	Description	Release Date
-	CR ESD-009	Initial Release (Reference CRD ESD-0009, dated 09/20/2012)	09/20/2012
A	CR ESD-0043	Revision A (Reference CR ESD-0043, dated 07/18/14) Summary of Changes: • Major revision of the ESD Safety & Mission Assurance Plan – entire document was open for review • Significant changes included updates to ESD S&MA Organization, removal of references to ESMAP • Expansion of Section 4.0 Safety, including major changes to Flight System Safety (Cross Program Integrated Hazard Analysis • Addition of Payload Safety and Human Rating sections	12/11/2014
B	CR ESD-0064-X	Revision B (Reference CR ESD-0064-X, dated 8/26/15) Summary of Significant Changes: • Split 5.0 into separate FMEA and PRA sections. • Closed TBD-10010-007, TBD-10010-008, TBD-10010-010, TBD-10010-013, TBD-10010-014 • Updated ITT responsibilities • Defined Tech Authority Flow • Defined Part B Exception Process • Defined Catastrophic • Removed Green, Yellow, Red from Hazard acceptance matrix. Replaced with zones. • Updated description of S&MA organization • Revised Ground Processing Safety to clarify the roles of GSDO Safety and IHAITT in integrated hazards	03/03/2016

TABLE OF CONTENTS

SECTION **PAGE**

1.0 INTRODUCTION 6
1.1 PURPOSE 6
1.2 SCOPE 6
1.3 CHANGE AUTHORITY/RESPONSIBILITY 7
2.0 DOCUMENTS 7
2.1 APPLICABLE DOCUMENTS 7
2.2 REFERENCE DOCUMENTS 8
3.0 MANAGEMENT AND ADMINISTRATION 10
3.1 SAFETY AND MISSION ASSURANCE TECHNICAL AUTHORITY 10
3.2 SAFETY AND MISSION ASSURANCE ORGANIZATION 10
3.3 S&MA INTEGRATION 15
3.4 INTEGRATED S&MA PRODUCTS 18
3.5 S&MA REQUIREMENTS 18
3.6 EVALUATIONS AND RESOLUTION OF ISSUES 19
3.7 INTEGRATION ASSURANCE 19
3.8 BUDGET AND RESOURCES 20
3.9 S&MA IN THE CAPABILITY-DRIVEN FRAMEWORK 20
4.0 SAFETY 20
4.1 SYSTEM SAFETY 20
4.2 GROUND PROCESSING SAFETY 38
4.3 RANGE SAFETY 39
4.4 PAYLOAD SAFETY 39
4.5 INDUSTRIAL SAFETY 39
4.6 MISHAP PREPAREDNESS AND CONTINGENCY PLAN 40
4.7 ORBITAL DEBRIS ASSESSMENT 40
5.0 RELIABILITY AND FAILURE MODES 41
5.1 FMEA/CIL INTEGRATION TASK TEAM 41
5.2 COMMON FMEA CONTENT 42
5.3 SYSTEM RELIABILITY PREDICTIONS 43
6.0 QUALITY ASSURANCE 43
6.1 PROBLEM REPORTING AND DISPOSITION 43
6.2 DATA REQUIREMENTS FOR HARDWARE HAND-OVER 44
6.3 SUPPLIER AUDITS 44
6.4 GOVERNMENT MANDATORY INSPECTION POINTS (GMIPS) 45
6.5 QUALITY INTEGRATED TASK TEAM 46
7.0 ESD PROBABILISTIC RISK ASSESSMENT 46

8.0 PROGRAM RISK MANAGEMENT 51

9.0 CERTIFICATIONS 51

9.1 HUMAN-RATING 51

9.2 CERTIFICATION OF FLIGHT READINESS (CoFR) 52

APPENDIX

APPENDIX A ACRONYMS, ABBREVIATIONS, AND GLOSSARY OF TERMS 53

APPENDIX B OPEN WORK 57

APPENDIX C SAFETY TOPICS 59

APPENDIX D MILESTONE REVIEW SUCCESS CRITERIA FOR ESD INTEGRATED HAZARD ANALYSIS 65

APPENDIX E CONTENT AND MATURITY CRITERIA FOR THE CROSS PROGRAM CREW SURVIVAL ANALYSIS REPORT 68

APPENDIX F CLARIFICATION OF FAILURE TOLERANCE APPLICABILITY TO HAZARD CAUSES 72

APPENDIX G CROSS PROGRAM MATERIAL REVIEW BOARD CHARTER 75

TABLE

TABLE 2.1-1 APPLICABLE DOCUMENTS 7

TABLE 2.1-2 REFERENCE DOCUMENTS 8

TABLE 3.2-1 S&MA PROGRAM AND TECHNICAL AUTHORITY RESPONSIBILITIES 12

TABLE 3.2-2 S&MA MANAGEMENT 13

TABLE 3.3-1 S&MA INTEGRATED TASK TEAMS 16

TABLE 5.2-1 CRITICALITY CATEGORY DEFINITIONS 42

TABLE B1-1 TO BE DETERMINED ITEMS 57

TABLE B2-1 TO BE RESOLVED ISSUES 57

TABLE B3-1 FORWARD WORK 58

TABLE E-1 CSAR CONTENT AND MATURITY CRITERIA FOR SRR/SDR 68

TABLE E-2 CSAR CONTENT AND MATURITY CRITERIA FOR PDR 69

TABLE E-3 CSAR CONTENT AND MATURITY CRITERIA FOR CDR 70

TABLE E-4 CSAR CONTENT AND MATURITY CRITERIA FOR DCR/ORR 71

TABLE F-1 HAZARD CAUSES THAT ARE EXCEPTED FROM FAILURE TOLERANCE BASED ON NPR 8705.2B 73

FIGURE

FIGURE 4.1-1 ESD HAZARD RISK ACCEPTANCES 30

FIGURE 4.1-2 HAZARD LIKELIHOOD DEFINITIONS 31

FIGURE 4.1-3 HAZARD SEVERITY DEFINITIONS 32

FIGURE 4.1.6.1-1 PART B EXCEPTION PROCESS 34

FIGURE 6.4-1 CROSS PROGRAM – GMIP PROCESS 45

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this plan is to define the approach for integrating the safety, reliability, and quality assurance activities throughout the Programs within the Exploration Systems Development (ESD) Enterprise. It explains the integration of Safety and Mission Assurance (S&MA) analyses and activities among the Programs to assure the safety and success of integrated missions.

Each Program is expected to establish policies and requirements to fulfill the responsibilities agreed upon and documented in this plan. If any Program is unable to fulfill its agreed upon responsibilities, changes to the multi-Program agreements will be reflected as changes to this Plan. This Plan does not create the requirement for a Program to perform an activity, but this Plan is the documentation of agreements.

This Plan defines the S&MA interfaces between the Programs, as well as between the Program and Headquarters (HQ) Office of Safety and Mission Assurance (OSMA) and ESD. This Plan, together with the individual Program Plans listed in Section 2.2, responds to the National Aeronautics and Space Administration (NASA) requirement for a Program S&MA Plan identified in NPR 8715.3C, NASA General Safety Program Requirements (paragraph 1.5), and NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, Appendix G - Program Plan Template, 3.2, Safety and Mission Assurance Plan.

This is a living Plan that will be modified as needed to reflect the direction of Exploration Systems Development as part of the capability-driven framework. With the recognition that the development of exploration capabilities is based on a flexible path to multiple destinations, S&MA's approach to integration will need to be flexible as well.

1.2 SCOPE

This Plan addresses integrated Safety and Mission Assurance for Space Launch System (SLS) Program, Orion Multi-Purpose Crew Vehicle (MPCV) Program, and the Ground Systems Development and Operations (GSDO) Program. Only integrated activities are addressed. Each ESD Program is required to have a separate S&MA Plan to address stand-alone activities. Program S&MA Plans are identified in Section 2.2. Program S&MA Plans are a necessary component of the total S&MA planning for integrated missions and should be considered as technically linked with this integration plan. The focus of initial S&MA planning is to address the needs of the tactical capability (as defined in ESD 10012, ESD Concept of Operations). Although many aspects of the S&MA Plan are extensible to future missions and strategic paths, the Plan will be updated to adjust to changing strategic directions.

It is the responsibility of the Programs to ensure their individual Program S&MA activities address the integrated cross Program S&MA activities identified in this Plan.

1.3 CHANGE AUTHORITY/RESPONSIBILITY

Proposed changes to this document will be submitted via a Change Request (CR) to the Exploration Systems Development Control Board (ECB) or delegated board or panel for consideration and disposition.

All such requests will adhere to the ESD Configuration Management Change Process (ESD 10005).

The System Safety Functional Area Lead (FAL) under the ESD Cross Program Systems Integration (CSI) Cross Program Integration Team (CPIT) maintains this Plan. The Office of Primary Responsibility (OPR) identified for this document is CSI.

Cognizant Programs, which retain change authority for those plans, are responsible for maintaining the Program S&MA Plans.

2.0 DOCUMENTS

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.

TABLE 2.1-1 APPLICABLE DOCUMENTS

Document Number	Document Revision	Document Title
ESD 10001	Rev C	ESD Implementation Plan
ESD 10005	Rev B	ESD Configuration and Data Management Plan (CDMP)
ESD 10007	Rev C	ESD Systems Engineering Management Plan (SEMP)
ESD 10011	Rev A	Cross Program Probabilistic Risk Assessment Methodology
GSDO-RQMT-1114		Cross Program Launch Commit Criteria
NASA-STD-8709.20		Management of Safety and Mission Assurance Technical Authority (S&MA TA) Requirements
NM 7120-81		NASA Space Flight Program and Project Management Requirements
NPD 8700.1E		NASA Policy for Safety and Mission Success
NPR 7120.5	Rev E	NASA Space Flight Program and Project Management Requirements
NPR 8000.4		Agency Risk Management Procedural Requirements
NPR 8621.1		NASA Procedural Requirements for Mishap and Close Call

Document Number	Document Revision	Document Title
		Reporting, Investigating, and Recordkeeping
NPR 8705.2B	Rev B	Human-Rating Requirements for Space Systems
NPR 8705.5A	Rev A	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects
NPR 8705.6		Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments
NPR 8715.3C	Rev C	NASA General Safety Program Requirements
NPR 8715.5A	Rev A	Range Flight Safety Program
NPR 8715.6A	Rev A	NASA Procedural Requirements for Limiting Orbital Debris

2.2 REFERENCE DOCUMENTS

TABLE 2.1-2 REFERENCE DOCUMENTS

Document Number	Document Revision	Document Title
SLS-RQMT-216		EM-1 Safety Requirements for Secondary Payload Hardware
SLS-PLAN-217		EM-1 Secondary Payloads Safety Panel Process
ESD 10002	Rev D	ESD Requirements
ESD 10004 <TBD-10010-015>		ESD Mishap Preparedness and Contingency Plan
ESD 10003	Rev C	ESD Risk Management Plan
ESD 10009		Human Rating Certification Package
ESD 10012	Rev C	ESD Concept of Operations
ESD 10114		ESD Range Safety
ESD 10015		ESD Systems Safety Analysis Report
ESD 10020 <TBD-10010-016>		ESD Certification of Flight Readiness (CoFR) Plan
ESD 20001	Version 2	ESD Cross Program Failure Modes and Effects Analysis Integration Summary Report
GSDO-PLN-1000		Ground Systems Development and Operations (GSDO) Program Plan
GSDO-PLN-1027		Cross Program Ground Hardware / Software Acceptance Data Package

Document Number	Document Revision	Document Title
GSDO-PLN-1036		Ground Systems Development & Operations Safety & Mission Assurance Plan
GSDO-PLN-1143		Cross-Program Flight Hardware / Software Acceptance Data Plan
GSDO-PLN-1055		Cross-Program Ground Hardware Integration Plan
GSDO-PLN-1073		Cross Program Launch Site Integrated Test and Checkout Plan
GSDO-PLN-1076		Cross Program Operations and Maintenance Requirements Specifications Management Plan
GSDO-PLN-1083		GSDO Mishap Preparedness and Contingency Plan (MPCP)
MIL-STD-882		System Safety Program Requirements
MPCV 70146		MPCV ADP Requirements
MPCV 72008		Orion Program Plan
MPCV 72094		Orion Safety & Mission Assurance Plan
MPCV 72223		Orion Mishap Response and Contingency Action Plan
MPCV 72532	Rev A	Orion Multi-Purpose Crew Vehicle Program Crew Survival Analysis for EM-2 Reference Mission
NASA Reference Publication 1358		System Engineering “Toolbox” for Design-Oriented Engineers
NASA/SP-2010-576		NASA Risk-Informed Decision Making Handbook
NASA/SP-2011-XX		NASA Risk Management Handbook
NASA-HDBK-8719.14A		Handbook for Limiting Orbital Debris
NPD 1000.1		NASA Strategic Management Handbook
NPD 7120.5		NASA Requirements for Program and Project Management
NPD 8700.1	Rev E	NASA Policy for Safety and Mission Success
NPR 8705.6		Safety and Mission Assurance (SMA) Audits, Reviews, and Assessments
SAE ARP4761		Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
SLS-PLAN-001		Space Launch System (SLS) Program Plan
SLS-PLAN-013		Space Launch System Program Safety & Mission Assurance Plan

Document Number	Document Revision	Document Title
SLS-PLAN-117		Space Launch System Program Mishap Preparedness and Contingency Plan (MPCP)
SLS-RQMT-014		SLS S&MA Requirements

3.0 MANAGEMENT AND ADMINISTRATION

3.1 SAFETY AND MISSION ASSURANCE TECHNICAL AUTHORITY

In accordance with NPD1000.1, NASA Strategic Management Handbook, and NPR 7120.5, NASA Requirements for Program and Project Management, NASA has implemented the S&MA Technical Authority (TA) governance strategy for ESD Programs. The Chief of NASA Headquarters (HQ) Office of Safety and Mission Assurance (OSMA) delegates the Program S&MA technical authority to the Center Director for the Program's host Center, who has further delegated authority to the Center S&MA Director. Each Center S&MA Director has in turn, identified a Chief S&MA Officer (CSO) for each Program. (See Table 3.1-1)

In addition, NASA HQ OSMA requires an ESD CSO to execute the ESD level S&MA Technical Authority. It is important to note that the ESD CSO may physically reside at a NASA Center or HQ, and therefore the ESD CSO may reside within a specific center-based supervisory chain of command particular to that residence. However, the S&MA Technical Authority flows directly from the Chief OSMA to the ESD CSO. (See Table 3.1-1). Cross program issues requiring formal ESD level S&MA TA will flow upward along their respective and relevant TA paths, including relevant Center S&MA Directors and relevant Center Directors as well as ESD. The relevant Program CSOs and the ESD CSO are responsible for ensuring proper communication across relevant stakeholders and management chains.

Table 3.1-1 S&MA Tech Authority Flow

S&MA Technical Authority "Flow" for Center-Hosted Programs	S&MA Technical Authority "Flow" for ESD
• Chief OSMA • Center Director of Program's Host Center • Center S&MA Director of Program's Host Center • Program CSO	• Chief OSMA • ESD CSO

3.2 SAFETY AND MISSION ASSURANCE ORGANIZATION

The S&MA organization within each ESD Program is defined within each Program's S&MA Plans identified in Section 2.2. The S&MA organization at the ESD level consists of a multi-

center team performing cross program S&MA functions, assuring the acceptability of cross program content, and exercising ESD level S&MA TA.

ESD and ESD Programs have ownership and responsibility over the S&MA content required to execute their Programs and ESD responsibilities. Historically, the management of such S&MA content has resided within the “program” organizational structure, with the independent TA function residing outside of the “program” organizational structure (instead, residing within an institutional organization). However, for ESD and each ESD Program, the management of required S&MA content has been delegated to the respective CSO. The CSOs are still “independent” and still reside outside of the ESD/Program organizational structure. However, the CSOs also conduct the programmatic S&MA management function as a dual role. This dual role approach creates additional complexity and results in a dual TA versus S&MA management reporting path (plus additional supervisory chain of command reporting paths), with the TA function flowing along the TA path (see Table 3.1-1) and the S&MA management function flowing to the ESD Director or Program Manager depending upon respective CSO/counterpart.

The ESD CSO, together with the Program CSOs, form the management nucleus, which manages all S&MA functions within ESD and the ESD Programs. The ESD CSO and the Program CSOs are voting members of the ESD and Program boards and panels as defined in their respective charters.

TABLE 3.2-1 S&MA PROGRAM AND TECHNICAL AUTHORITY RESPONSIBILITIES

S&MA Program Management	S&MA Technical Authority
• Direct and control ESD S&MA • Serve as member of ESD teams and control boards (CPIT, JICB, JPCB, ECB, QPSR) to assure compliance with S&MA Technical Authority requirements and concur on the acceptability of residual safety risk • ESD S&MA requirement development • Manage ESD S&MA budget/resource (cost authority) • Manage/oversight ESD S&MA product development (schedule authority) • Manage ESD Quality Management System (QMS) • Status reports, metrics, and risk reports for ESD S&MA Work Breakdown Structure (WBS) • Ensure Integrated S&MA risks are identified, characterized, and resolved appropriately • Ensure all ESD S&MA integration tasks are planned and accomplished • Support to Chief OSMA, ESD Director, etc. • Directing and controlling the S&MA elements of the Program • Program/project S&MA requirement development • Prime contract Statement of Work (SOW)/Data Requirements development and performance evaluation • S&MA budget/resource management (cost authority) • Management/oversight of S&MA product development (schedule authority) • Management of program/project Quality Management System (QMS) • Status reports, metrics, and risk reports for S&MA Work Breakdown Structure	• Serve as member of ESD teams and control boards (CPIT, JICB, JPCB, ECB, QPSR) to assure compliance with S&MA Technical Authority requirements and concur on the acceptability of residual safety risk • Provide concurrence on the technical suitability of S&MA products provided for ESD approval • Assure proper flow down and application of S&MA Technical Authority requirements, provide interpretation of such requirements as needed • ESD S&MA requirement development • Assure that requests for waivers or deviations from Technical Authority requirements are submitted to and acted upon by the appropriate level of Technical Authority • Ensures Integrated S&MA risks are identified, characterized, and resolved appropriately • Assure proper disposition of Dissenting Opinions • Support to Chief OSMA, ESD Director, etc. • Serving as member of program or project control boards, change boards, and internal review boards to assure compliance with S&MA Technical Authority requirements and concur on the acceptability of residual safety risk • Provide concurrence on the technical suitability of S&MA products provided for program/project approval • Assuring proper flow down and application of S&MA Technical Authority requirements and providing interpretation of such requirements as needed • Program/project S&MA requirement

S&MA Program Management	S&MA Technical Authority
	development • Assuring that requests for waivers or deviations from Technical Authority requirements are submitted to and acted upon by the appropriate level of Technical Authority • Assuring proper disposition of Dissenting Opinions

TABLE 3.2-2 S&MA MANAGEMENT

Position	ESD Responsibilities	Primary Customers
ESD CSO	○ Exercise S&MA TA for ESD ○ Serve as member of ESD teams and control boards (CPIT, JICB, JPCB, ECB, QPSR) to assure compliance with S&MA Technical Authority requirements and concur on the acceptability of residual safety risk ○ ESD S&MA requirement development ○ Ensure Integrated S&MA risks are identified, characterized, and resolved appropriately ○ Provide concurrence on the technical suitability of S&MA products provided for ESD approval ○ Assure proper flow down and application of S&MA Technical Authority requirements, provide interpretation of such requirements as needed ○ Assure that requests for waivers or deviations from Technical Authority requirements are submitted to and acted upon by the appropriate level of Technical Authority ○ Assure proper disposition of Dissenting Opinions ○ Direct and control ESD S&MA ○ Manage ESD S&MA budget/resource (cost authority)	• Chief OSMA • ESD Director

Position	ESD Responsibilities	Primary Customers
	○ Manage/oversight ESD S&MA product development (schedule authority) ○ ESD S&MA requirement development ○ Ensure Integrated S&MA risks are identified, characterized, and resolved appropriately ○ Manage CSI S&MA integrated product list assurance function ○ Manage ESD Quality Management System (QMS) ○ Status reports, metrics, and risk reports for ESD S&MA Work Breakdown Structure (WBS) ○ Ensure all ESD S&MA integration tasks are planned and accomplished ○ Represents ESD S&MA in the CPIT	
Program CSO	• Program S&MA Technical Authority ○ S&MA Rep to Program Control Board (PCB) • Program's S&MA management • Ensure Program's ESD integration tasks and products are accomplished per agreed-to technical scope and schedule	• Respective Center S&MA Director • NASA Chief of S&MA • Program Manager • ESD CSO • Program Chief Engineer

Position	ESD Responsibilities	Primary Customers
ESD System Safety Functional Area Lead (FAL)	• Ensuring ESD integrated System Safety products are completed and delivered • Maintaining the ESD S&MA Plan • Coordinating with the ESD and Program CSOs on the resolution of issues associated with Cross Program System Safety tasks and products • Maintaining System Safety Integrated Task Team (ITT) Task Agreements • Identifying and resolving impacts resulting from proposed changes to System Safety Task Agreements or changes to the System Safety functional area construct • Communicating risks and issues to the Integration and Program CSOs where safety and mission success may be impacted • Coordinating with ESD CSO, CPIT, and affected System Safety ITT Leads to manage the response to actions, questions, or findings affecting S&MA in multiple human exploration programs originating from joint program management forums, independent reviews, internal and external peer reviews, or external oversight review panels	• ESD CSO • Program CSO's • ESD Chief Engineer • Cross Program Integration Team (CPIT) Leadership

3.3 S&MA INTEGRATION

The ESD/CSI Cross Program Integration Team (CPIT) provides the leadership for cross program technical integration as described in ESD 10007, ESD System Engineering Management Plan (SEMP). The ESD CSO is the S&MA member of the CPIT.

In the CPIT construct, multiple Integrated Task Teams (ITTs) perform cross program integration tasks. These ITTs are logically organized into functional areas under CPIT leadership as described in the ESD SEMP (ESD 10007). Each functional area is managed by a Functional Area Lead (FAL) charged with responsibilities as described in the SEMP.

One of these functional areas is System Safety, which includes the ITTs tasked to provide the system safety-related analytical planning products needed for cross program integration. In addition to the general responsibilities of FALs documented in the ESD SEMP, the System Safety Functional Area Lead (FAL) has those responsibilities listed in table 3.2-2.

The System Safety ITTs (SS ITTs) are comprised of subject matter experts from each affected Program and ESD as needed. These ITTs collaborate on specific integrated products and processes to determine the need for commonality of products or processes, the appropriate governing requirements/agreements, data exchange requirements, and program responsibilities. The ITTs manage the execution of the integrated activities and the development of the integrated products.

The SS FAL, working with the SS ITT leads, will document and maintain task agreements that describe SS ITTs' scope, tasks, products, membership, and relevant schedules. These task agreements are approved by the CPIT. The ESD CSO will coordinate with Program CSOs and the System Safety Functional Area Lead prior to concurring on ITT task agreements affecting program S&MA resources or activities. The current SS ITTs are identified in Table 3.3-1.

TABLE 3.3-1 S&MA INTEGRATED TASK TEAMS

Integrated Task Teams	Responsibilities	Lead
Integrated Hazard Analysis ITT (IHAITT)	• Define the Cross Program Integrated Hazard Analysis (CPIHA) process • Develop the CPIHA • Manage the CPIHA approval and risk acceptance process • Integrate with other ITTs, including the Cross Program Probabilistic Risk Assessment and Failure Modes & Effects Analysis/Critical Items List (FMEA/CIL) and Crew Survival Analysis integration teams	ESD
Cross Program Probabilistic Risk Assessment Team (XPRAT)	• Support Level I requirement development • Establish Probabilistic Risk Assessment (PRA) methodology • Develop the ESD Integrated PRA • Manage the ESD Integrated PRA reporting and risk mitigation process • Integrate with IHAITT • Cross Program Loss of Crew (LOC)/Loss of Mission (LOM) verification • Analyze LOC, LOM, and Loss of Orion MPCV for various Design Reference Missions (DRM)	Orion MPCV

Integrated Task Teams	Responsibilities	Lead
Quality Integrated Task Team (QuITT)	• Determine Quality Assurance (QA) requirements for Hardware /Software handover and manage related QA processes • Develop and manage closed-loop process for SLS/Orion Government Mandatory Inspection Points (GMIPs) in GSDO to ensure GMIPs are assigned and closed-looped tracked for SLS and MPCV once the hardware is turned over to GSDO (KSC) • Develop and manage inter-program Problem Reporting and Corrective Action System (PRACA) process • Develop and manage an integrated audit strategy • Manage ESD Acceptance Data Package (ADP) (TBR)	SLS
Cross Program Failure Modes and Effects Analysis Integrated Task Team (CP FMEA/CIL ITT)	• Review and impact Program FMEA/CILs to assure that the risk associated with failure mode effects that cross a Program-to-Program interface is well understood, controlled, and accepted by the Programs on both sides of the interface • Coordinate the sharing of Program FMEA/CILs to ensure all integrated failure effects are properly identified and resolved • Develop and release ESD 20001 Cross Program Failure Modes and Effects Analysis Integration Summary Report • Integrate with ESD IHA	SLS

Integrated Task Teams	Responsibilities	Lead
Crew Survivability Assessment	• Develop the Crew Survival Analysis Report which identifies the available crew survival capabilities across the DRM phases and highlights any gaps in crew survival capabilities for possible mitigation or risk acceptance by the various programs • Provide the necessary documentation for the Human Rating Certification Package (HRCP) to show compliance with the human rating requirements (NPR 8705.2B) relative to crew survival • Track and coordinate open work items necessary to verify and validate the implementation of crew survival capabilities • Facilitate the integration of Crew Survival Methods into the Hazard Analysis process	Orion MPCV

3.4 INTEGRATED S&MA PRODUCTS

The CPIT oversees the development of ESD-level and integrated products that drive cross program integration, including the in-line products developed under the System Safety functional area. These products are described in the CPIT's Integrated Product List (IPL).

The SS ITTs manage the development of S&MA products on the IPL, excluding this ESD S&MA Plan, which is managed by the SS FAL. This includes the establishment and maintenance of schedules for interim and final product deliveries.

3.5 S&MA REQUIREMENTS

NASA Headquarters Office of Safety and Mission Assurance levies NASA safety and mission assurance policies, requirements, and standards on ESD and each Program. ESD and each Program, through an agreed upon process, will evaluate the OSMA applied S&MA Technical Authority (TA) requirements and resolve applicability, tailoring, or exceptions/deviations with Program management, Center S&MA, and OSMA. The Program CSO is responsible for assuring the appropriate S&MA TA requirements are determined, applied on the Program, and traceable to Program requirements and contracts, and any exceptions or deviations have been appropriately resolved.

The ESD CSO is responsible for assuring the appropriate S&MA TA requirements are determined, applied on ESD, and traceable to ESD requirements, and any exceptions or deviations have been appropriately resolved.

Each Program will have S&MA requirements documented in Program-controlled documentation. There will not be an ESD integrated S&MA requirements document applied on all three Programs.

Requests for variance from OSMA requirements are handled as described by NPR 8715.3C, paragraph 1.13.

3.6 EVALUATIONS AND RESOLUTION OF ISSUES

The ESD CSO, working with the Program CSOs and others, will maintain cognizance of cross program technical and programmatic risks and issues with potential ramifications for safety and mission success. The CSOs will collectively evaluate these items to establish a unified S&MA Technical Authority position. The CSOs will solicit and hear any dissenting opinions. If consensus for a single S&MA TA position is reached, that position will be communicated to ESD and Program management via the appropriate forums. Where there is a dissenting opinion, and the owner wishes to elevate it, he or she will be invited to voice that opinion at those forums. The responsible CSO (ESD or Program) will facilitate the resolution of any dissenting opinions.

Generally, the ESD CSO will provide the S&MA TA position at ESD and joint Program management forums. For joint integration forums, the CSOs will decide which CSO communicates the S&MA TA position.

3.7 INTEGRATION ASSURANCE

In addition to the in-line tasks and products performed as part of the integration activities, Exploration Systems Integration (ESI) has a role in assuring the performance and outputs of critical activities. S&MA cannot and should not provide assurance on every activity and product, so a risk informed decision-making approach is employed to determine where and how S&MA engages cross program integration.

Periodically, the ESD and Program CSOs review the following to determine the degree of S&MA engagement needed and to make or adjust assignments of Program and CSI S&MA resources as needed to ensure the appropriate coverage.

- ITT list and activities
- CPIT top issues
- ESD Top risk list
- Planned change requests
- Issues arising from the System Safety functions

The ESD CSO collaborates with the Program CSOs to maintain an assignment matrix for S&MA personnel engaging the ITTs, CPIT functional areas, or other integration teams and activities. Generally, Programs will provide resources necessary to ITT-level assurance, while the ESD CSO provides assurance of the CPIT functional areas. However, the CSOs will adjust the assurance responsibilities as needed to promote effectiveness and efficiency.

3.8 BUDGET AND RESOURCES

Each Program budgets for S&MA resources, as well as the associated engineering and institutional resources, to fulfill its responsibilities as defined by this plan. Some resources, such as databases, may be shared among the Programs and funding is arranged on a case-by-case basis.

The responsibilities of the System Safety FAL, as well as any technical or administrative support required by the FAL or the ESD CSO, are funded by ESI. ESI may also, at its discretion, fund specific S&MA analyses or activities unrelated to the System Safety FAL (e.g. risk assessments in future mission studies).

3.9 S&MA IN THE CAPABILITY-DRIVEN FRAMEWORK

The capability-driven framework creates an expectation of systems development to support multiple possible future missions. As such, the S&MA processes must support current systems development activities, while also being flexible to adjust to strategic changes in the future as decisions are made. S&MA design analysis work (hazard analysis, Failure Modes and Effects Analysis (FMEA), PRA on initial ESD systems for the tactical capability) will assume the EM-1 and EM-2 Design Reference Missions (DRMs).

The majority of hazard analysis and FMEA work identifies failures and consequences of hardware/software systems and such scenarios are not dependent on the mission. The ability of the hazard analysis and FMEA to influence the design is still possible even without a confirmed mission or missions. This is particularly true for SLS and GSDO where systems and operations are largely common across multiple missions.

FMEAs are performed on system and component designs. The failure effects are described at multiple levels, including the effects on the mission and crew. FMEAs may require updates over time to incorporate new or different missions and mission effects. These updates may or may not change the risk or acceptability of critical items for the chosen missions, but re-evaluation of critical items by Program management will be conducted when such risk changes occur.

While specific missions and operations can introduce new hazards, a portion of the hazard analysis is based on identifying system failures as hazard causes. The hazard analysis can still influence system design for these causes as part of the capability-driven framework. As specific missions are defined, the hazard analysis will be updated for each flight to reflect flight-specific hazards that may arise.

4.0 SAFETY

4.1 SYSTEM SAFETY

4.1.1 System Safety/Hazard Analysis Process

Each ESD program is required to establish a system safety analysis and engineering process, which includes hazard analysis requirements in compliance with Agency NASA Procedural

Requirements (NPRs). This process should be documented in individual program S&MA plans and be consistent with the Program responsibilities delineated in this section.

ESD manages the cross program integrated hazard analysis process and products. The Cross Program Integrated Hazard Analysis (CPIHA) is a coordinated effort by all programs to analyze the hardware interfaces, system interactions, and interdependencies to identify the Cross Program Integrated Hazards (CPIHs), causes, effects, controls and verifications.

The CPIHA will provide the controls necessary to manage or mitigate the risk crossing the interface and assess the impact or effects of the residual risk between programs. The CPIHA is formally documented in ESD 10015, ESI System Safety Analysis Report (SSAR). Detailed process information is located at the Integrated Hazard Analysis ITT (IHAITT) wiki.

4.1.2 Cross Program Integrated Hazard Analysis Approach & Methodology

4.1.2.1 CPIHA Roles & Responsibilities

CPIHs require more than one program to contribute to the analysis, the interactions/interfaces, or interdependencies of the hazard. The Integrated Hazard Analysis ITT (IHAITT) is responsible for the CPIHA process. (See IHAITT Task Agreement for membership and other details.) The IHAITT actively manages the development of the Cross program Integrated Hazard Analysis and is responsible for tracking the schedule and status of the CPIH content. The IHAITT is responsible for developing an IHA that has content that is technically accurate and at a maturity level that is consistent with program life cycle. A hazard that is not a CPIH by definition is a Program-only hazard. The CPIHA will identify and document the controls necessary to manage or mitigate the risk crossing the interface and assess the impact or effects of the residual risk between programs.

All stakeholders are provided access to meetings and any information maintained by the IHAITT for full visibility of the IHA process and results. If any stakeholder disagrees with IHAITT decisions or results, the concern can be addressed with the IHAITT, System Safety Area Functional Lead or elevated to higher forums (e.g. CPIT, JPCB, ESD CB) as required for resolution.

4.1.2.2 Definition of a Cross Program Integrated Hazard

A Cross Program Integrated Hazard (CPIH) is defined as any hazard occurring within the timeframe defined in section 4.1.2.3 in which more than one program is a contributing cause or control for the hazard. CPIH causes are causes for which controls are outside any one program or controls that involve Cross Program Integrated Hazard Analysis. The effects of a hazard may cross program interfaces but are not considered a CPIH. For example, catastrophic failure of the SLS affects the MPCV and the flight crew. However if both the hazard cause and controls are entirely within SLS, then it is a program only hazard. A hazard that is not a CPIH by definition is a Program Only Hazard.

4.1.2.3 Scope of the CPIHA

Hazard Analysis is performed at the Program and Cross Program Level, and addresses design and operational hazards associated with flight and ground hardware, software, operations, training, maintenance, and environments (including facilities) used in the successful execution of all baselined design reference missions.

The ESI CPIHA timeframe begins with the start of cryogenic loading operations at the pad and ends with post-flight crew egress. Hazards that potentially manifest within this timeframe are within scope of the ESI CPIHA if either of the following apply:

- The cause was introduced during integrated analysis or design processes due to process errors or deficiencies. This includes the development of integrated ground and flight operational requirements that may result in errors in operational procedures.

- The cause originated after the beginning of cryogenic loading operations.

The GSDO Program is responsible for developing and processing hazards due to causes introduced during ground operations prior to cryogenic loading and after post-flight crew egress with participation with Orion MPCV and SLS as required. However, during the roll-out phase of operation, the lightning hazards and roll-out loads hazards will be brought to a JPCB for final approval.

As part of the ESD S&MA assurance role, the IHAITT in conjunction with the affected programs will review these causes and determine if they need to be elevated to the CPIHA or remain within a particular program. The CPIHA is initially performed for baselined missions (EM-1 and EM-2). It will be updated as additional design reference missions are added to the baseline. The programs will also review their causes and can propose any cause they determine meet the CPIHA criteria to be elevated to the CPIHA.

Emergency systems will be analyzed for integrated hazards associated with their existence. (e.g., Launch Abort System (LAS) inadvertent operation). Hazard analysis will not be performed on emergency equipment in emergency or crew survival operations.

Assets and operations owned and operated by agencies external to ESD (e.g. Department of Defense) are not included in the CPIH. Interfaces and operations between an external entity and a single program are assessed for potential hazards per that program's processes. The CPIHA assesses potential hazards involving multiple program and external agencies where the definitions cited in 4.1.2.2 apply. CPIHA analyzes ESD hazard causes that may affect external agencies and hazard controls that may be required from external agencies. Interface and integration requirements are established with external agencies to define safety requirements, responsibilities, and review processes

4.1.2.4 CPIHA Format and Data Management

While each program may have program-unique requirements for hazard product format or content, CPIHA products (hazard cause trees and causes) are developed based on the

common set of guidelines described in this plan. CPIHA products are documented using a common set of hazard database fields.

The CPIHA causes and cause trees are data managed by the IHAITT within a controlled access hazard analysis database. CPIH results and products are documented in ESD 10015, SSAR.

4.1.2.5 Information Sources

Information sources which aid identification of CPIHs include (but are not limited to): concept of operations, integrated mission and functional analyses, generic/standardized hazard identification checklists, prior failure history, DRMs; mission timelines, flight test objectives, hardware/Ground Support Equipment (GSE) designs, individual program hazard reports, Interface Requirements Documents (IRDs), Interface Control Documents (ICDs), Space Shuttle or Constellation fault trees, hazard analyses, FMEA/CILs, and PRA models.

4.1.2.6 Integrated Hazardous Conditions

Top-level hazardous conditions are identified based on the information sources listed above. The CPIHA, performed with participation from all Programs' engineering and safety organizations, determines a preliminary list of cross program integrated hazardous conditions for the ESD Design To Sync (DTS) milestone. Other stakeholders including flight crew, mission operations, and Human Health and Performance (HHP) also provide input to the CPIHA. The list of integrated hazardous conditions will be updated as necessary due to design maturity or design/operational concept changes.

4.1.2.7 Integrated Hazardous Causes

Cause trees will be developed from the list of integrated hazardous conditions. The cause trees are used to identify the CPIH causes for each integrated hazardous condition. CPIH causes will be assigned to the accountable program to be developed with engineering and safety technical authority representatives (or their designees) from the affected programs to define controls and verifications. Any causes determined to be program-only will be passed to the identified program for further evaluation. Individual programs are responsible for verification assuring that program-only hazard causes have been properly addressed.

The Program engineering and S&MA representatives to the IHAITT assign S&MA and Engineering representatives to be responsible for the collaborative effort to generate and develop each CPIH cause. Engineering is accountable for identifying the cause effect and design mitigation strategy, including controls and verifications. S&MA provides hazard analysis process expertise and will ensure completeness by assuring all the controls, verifications, severities, and likelihood have been addressed. In addition, S&MA will coordinate with the other program stakeholders (Crew, Operations, HHP) as required concerning other risk mitigation strategies (crew survival or operations options). Mission operations, as well as Crew and HHP are accountable for working with S&MA and engineering to ensure any operations controls are credible and can be implemented.

Acceptance rationale will be developed at the cause level. The CPIHA will identify CPIH causes throughout the lifecycle of the programs as needed to reflect changes in designs and operations.

4.1.2.8 Integrated Hazard Controls

Hazard cause controls will be identified for each cause to address the associated hazard. In many cases existing cross program design or operational requirements contain the necessary controls, however, new requirements will be added to ICDs, Interface Requirements Document (IRDs), operational documentation, program design specifications, etc., as necessary to implement the required hazard controls. Hazard analyses will maintain traceability to controls documented in requirements and design specifications. Traceability will be maintained between hazard causes and the formal documentation where the controls actually reside.

4.1.2.9 Hazard Control Verification

Verification activities will demonstrate that risk mitigation and hazard controls have been implemented. Each cause identifies preliminary hazard control verification plans at Preliminary Design Review (PDR), with final verification plans at CDR. For hazard verifications that are not complete by System Acceptance Review (SAR) or equivalent milestone, each program maintains a Safety Verification Tracking Log (SVTL) or equivalent for those verifications for which it is responsible. Prior to integrated ground or flight operations, the IHAITT ensures closure of all applicable CPIHA control verifications through audit and review of the SVTLs.

Hazard control verification is performed according to one of the following processes, with all verifications tracked as described above. Where applicable, hazard control verification uses existing ESD and Program verification processes.

a) Hazard control is implemented through a Program's design – verification is handled through the normal design verification process defined in each Program's V&V Plan and verification is through Inspection, Test, Demonstration and/or Analysis.

b) Hazard control is implemented through an Operational Control (e.g., flight rule, procedure, and training) – operational control verification is handled through the MOD Operational Control Agreement Document (OCAD) system (<TBD-10010-009>) for flight rules/procedures/training. The Cross program Operations and Maintenance Requirements and Specifications (OMRS) (GSDO-PLN-1076) and Cross program Launch Commit Criteria (LCC) (GSDO-RQMT-1114) processes are used for recurring safety hazard control verifications not handled through the design process described above.

c) Hazard control is implemented through a process that is not design and not an operational control (e.g., analysis) – verification is handled through the process defined within the specific hazard verification statement.

Programs ensure successful hazard control implementation using a methodology to track hazard controls and verifications both within a program and across multiple programs. The system at a minimum should include a "hazard control" identifier in program documentation, and

be traceable to the hazard product and the cause of the supporting program (a transfer in and a transfer out).

4.1.3 Hazard Risk Classification

Each CPIH and Program cause is assigned a likelihood and severity level using the likelihood and severity definitions in Figure 4.1-2 and Figure 4.1-3, respectively. Classification of risk will be based upon listed controls and verifications (as expected to be implemented).

Severe hazards do not apply to flight after T-0. Injuries to crew or occupational illness of crew in flight, which are more severe than “first aid” but do not result in permanent disability, are considered to result in loss of mission and therefore classified as “critical”. For the purposes of system safety design, injuries or illness that would normally require emergency medical care are considered catastrophic due to an expected lack of medical care resources in flight. Injuries to crew in flight, which result in permanent disability, are considered catastrophic. Damage to flight systems during in-flight operations, which, in the worst case, have no effect on the mission completion (i.e., not Loss of Mission) are classified as minor. Program Hazard Analysis Review

In accordance with NPR 8715.3, NASA General Safety Program Requirements, a safety review process will be used to assist each program in assuring that the safety analyses are compliant with applicable requirements, comprehensive, technically accurate and that residual risks are at acceptable levels. Each program will determine the type of safety review activity that will be performed. The review process description will reside in the respective Program’s S&MA plan. Establishing a safety review panel is not required; however, each program will ensure that the required stakeholders are included in the review and approval of the system safety analysis as shown below. The Program CSO will ensure that each program has a safety review activity that assures the accuracy and adequacy of the Hazard Analysis product prior to approval at the appropriate board.

The safety review activity will include an evaluation by safety and subject matter experts that were not responsible for developing the hazard products. To assure that safety risk is communicated to the appropriate stakeholders, the safety review process should consider, at a minimum, a representative from the following organizations:

- ESD
- S&MA Technical Authority
- Engineering Technical Authority
- Health & Medical Technical Authority
- Risk-takers (Crew Office and/or ground operators)
- Orion MPCV Program
- Ground Systems Development & Operations (GSDO) Program
- Space Launch System (SLS) Program
- Flight Operations Directorate (formerly Flight Crew Operations and Mission Operations)

4.1.4 Cross Program Integrated Hazard Analysis Review

Prior to any program or integrated milestone review, the IHAITT identifies portions of the overall CPIHA content applicable to that review and collects that content as part of the ESI System Safety Analysis Report (SSAR). The basic SSAR contents will include: a list of integrated hazardous conditions; cause trees; integrated causes; program cause accountability records; and a list of issues and watch items. The remaining contents of the SSAR may vary between milestones, but each SSAR dropped for ESI reviews will meet the success criteria documented in Appendix D. These criteria are provided in order to ensure that the maturity of CPIHA products is commensurate with the objectives of the review milestone.

Integrated hazardous causes (described in 4.1.2.7) constitute the primary content of the SSAR. Hazard causes applicable to a given Program or cross program milestone undergo a tabletop review (TTR) prior to incorporation into and release of the SSAR.

4.1.4.1 Tabletop Review (TTR)

The objective of the TTR is to provide an in-depth review of the integrated hazard causes and related CPIHA content by a team of stakeholder representatives who are not part of the CPIHA development team. The CPIT will coordinate the TTR among the stakeholders listed in 4.1.4. The IHAITT will release the SSAR to the stakeholders' representatives ahead of the TTR. Stakeholder representatives will be provided sufficient time to review the package and provide comments back to the IHAITT for discussion during the TTR. The IHAITT will convene the TTR, during which the IHAITT and stakeholders will discuss any outstanding comment dispositions and answer any further questions. The IHAITT Lead chairs the TTR and dispositions comments for incorporation into the CPIH products. The IHAITT Lead assigns actions as needed to resolve any open issues or close loops on remaining questions.

The Engineering and S&MA teams that develop the CPIHA products incorporate agreed-to-revisions into the products and close any actions that potentially constrain release of the products for upcoming milestones.

4.1.4.2 The CPIHA in Program Milestone Reviews

The CPIHA effort supports each program's milestones including design reviews and ESD Cross Program reviews as required. Given the varying states of design maturity and staggered timing of program-level milestone reviews across GSDO, Orion MPCV, and SLS, it is not likely that all the required elements of the integrated causes will be available or ready for review during any given program milestone in a series of common milestones. For example, if an SLS milestone review is scheduled some months before the corresponding GSDO milestone review, certain GSDO analyses or hazard-related information may not be available for inclusion in an SLS/GSDO integrated hazard cause for review during the SLS review. The IHAITT identifies those aspects of the CPIHA that are to be delivered to upcoming program milestones and schedule cause development and review accordingly.

Programs will establish a formal, closed-loop, risk acceptance process to identify and track hazards with residual risk, and communicate those risks for acceptance at each milestone review to assure that all hazards and risks identified in the CPIHA hazard analysis are either eliminated or controlled to acceptable levels. The other programs will be a part of the milestone review process to ensure complete identification of hazards, as well as correct controls and verifications related to those programs.

The “hosting” program will incorporate the integrated SSAR in their review products. Review teams may initiate comments (typically “Requests for Action”) per the program’s milestone review ground rules. Comments may be directed against the SSAR itself or against a program-owned product that may need to be corrected to accept the hazard cause. The IHAITT will participate in the program’s comment disposition forums to help direct comments to the IHAITT as necessary.

Each program milestone will include a briefing of program-only hazard products and any CPIHA products delivered for review summarizing the analysis effort, review process, open work or issues, and identifying any issues/risks as well as recommendations. The focused safety review of the hazard analysis presented to the Program Milestone Review Board (not a separate S&MA board but rather a programmatic board established to oversee a major review such as PDR, CDR, etc.) may be limited to hazard products which identify the high-risk levels. The presentation may include the control and verification strategy for the causes, the resulting safety risk, and the identified level of failure tolerance (including identification of any waivers that are required). The primary objective of such a briefing is to make the Board aware of high-risk items being identified by the hazard analysis or other known safety issues.

The IHAITT assumes the responsibility for the tracking and disposition of comments to the ESI SSAR. IHAITT will work with the programs as required to resolve all comments. The hosting program may elect to close these comments by noting the IHAITT’s responsibility. The IHAITT assures all comment resolutions receive concurrence from the initiators or are elevated to the appropriate forums for decision in the event of an inability to reach agreement with an initiator. The IHAITT will also report resolution status as necessary at subsequent milestones or other post-review forums.

Based on the results of the program milestone review, the IHAITT will update the SSAR in preparation for the next review.

4.1.4.3 The CPIHA in ESI Reviews

Following the completion of common program milestone reviews, the IHAITT will prepare the SSAR for a cross program review ahead of major ESD cross program reviews. Tabletop reviews may be convened as described in 4.1.5.1 in order to review updates and assure product readiness for the cross program review.

For ESD-led cross program milestones, the IHAITT will present the SSAR to the ECB for review before releasing it to the upcoming milestone review. Upon ECB concurrence, the IHAITT will deliver the SSAR to the cross program milestone review per the procedures for that review.

4.1.5 Residual Safety Risk Acceptance

Consistent with the NPD 1000, NASA Governance and Strategic Management Handbook; NPD 8700.1, NASA Policy for Safety and Mission Success; and the NPR 7120.5, NASA Space Flight Program and Project Management Requirements, the NASA Programmatic Authority has the responsibility to formally accept residual safety risks with the concurrence of the program Technical Authorities. Hazard products are used as a mechanism to fulfill this responsibility, and will be presented to Program Management, Cross Program Management, and the Technical Authorities for formal risks acceptance. The level of management required to approve the residual safety risks (including hazard risk products) and accept the residual safety risk level of the hazard is determined by the likelihood and consequence of the hazard as shown in Diagram 4.1-1. The residual safety risk acceptance matrix is divided into 4 zones. Program residual safety risks and hazards and CPIHs ending in zone 4 are brought to the NASA Administrator for acceptance. Program residual safety risk and hazards and CPIHs ending in zone 3 are brought to the ESD Control Board (ECB) for acceptance. Program residual safety risks and hazards ending in zone 2 are brought to the Program Control Board for acceptance, while residual safety risks and CPIHs ending in zone 2 are brought to the Joint Program Control Board for acceptance. The Program Manager may delegate interim approval of Program hazards ending in zone 2 but final acceptance of the residual safety risk must be by the Program Manager. Program residual safety risks and hazards and CPIHs ending in zone 1 are considered to have no significant residual risk and the Programs (and ESD) are not required to document hazards in zone 1. If the hazards in zone 1 are documented then they follow the same acceptance process as those in zone 2. ESD owns the integrated risk acceptance products, which the IHAITT manages. Hazard likelihood and severity definitions defined in Figure 4.1-2 and Figure 4.1-3, respectively.

It is important to note that the use of residual safety risk zones in Figure 4.1-1 in order to determine the level of management required for formal risk acceptance is meant to convey a more broad risk acceptance protocol than solely the hazard analysis process. Hazard analysis, with its clear use of the 5x5 matrix for formal risk appraisal and acceptance, is the core example used to illustrate this zone-based risk acceptance protocol; however, it is possible that significant residual safety risk could be accepted by other means and through other Program processes. Before hazard analysis baseline, all residual risk that has been accepted through Program processes should be considered when determining where the ‘X’ belongs in the 5 x 5 matrix and safety risk zone in the final hazard analysis. After hazard analysis baseline, specific PRACA (including unexplained anomalies and use-as-is dispositions), MRB dispositions, waivers/deviations, and other significant non-conformances could all be opportunities for increased residual safety risk acceptance at the Program level. It will be important for each Program CSO to monitor these specific additional areas for any instances of proposed significant increase of residual safety risk for acceptance up to ESD or beyond. Already core to the Program CSO function, each Program CSO is expected to assure that residual safety risks within their Programs are formally accepted via formal Program processes and that the outlined risk acceptance protocol is consistently applied to hazard analysis as well as the specific additional examples cited above. Potential other risk acceptance areas may exist as well, and it will be up to each Program and Program CSO’s judgment to assess the need to elevate or not, thereby assuring that risk acceptance “sneak circuits” do not exist which could allow significant residual safety risk to be accepted at a level lower than otherwise appropriate.

ESD's risk acceptance philosophy is governed by the following NPRs:

- NPR 8715.3 NASA's General Safety Program Requirements – All
- NPR 8715.5A Range Flight Safety Program – Public
- NPR 8705.2B Human-Rating Requirements for Space Systems - Flight

Governing Safety & Mission Assurance plans are shown in Table 4-1.

TABLE 4-1 GOVERNING S&MA PLANS

Activity	Governing S&MA Plan
Personnel Activities at Contractor Site	Activities that are outside of NASA operational control are covered by contract, as well as federal, state, and/or local requirements addressing personnel safety
Personnel Activities at NASA Center – non-Launch Related	Center Safety and Health Program
Personnel Activities at NASA Center – Pre-Launch and Launch	Center Safety and Health Program, GSDO Program S&MA Plan and ESD 10010, ESD S&MA Plan
Personnel Activities of civil service or onsite contractor Ground Personnel During Mission	Center Safety and Health Program
Crew Activities During Mission	ESD 10010, ESD S&MA Plan; ESD 10009, ESD Human Rating Certification

EXPLORATION SYSTEMS DEVELOPMENT HAZARD MATRIX

LIKELIHOOD	MINOR	MODERATE	SEVERE	CRITICAL	CATASTROPHIC
VERY HIGH					4
HIGH				3	
MODERATE			2		
LOW		1			
VERY LOW					

SEVERITY

FIGURE 4.1-1 ESD HAZARD RISK ACCEPTANCES

PER MISSION	LIKELIHOOD	
	VERY HIGH	**QUALITATIVE: VERY LIKELY TO HAPPEN. CONTROLS ARE INSUFFICIENT.** **QUANTITATIVE: ~1/200 <P**
	HIGH	**QUALITATIVE: LIKELY TO HAPPEN. CONTROLS HAVE SIGNIFICANT LIMITATIONS OR UNCERTAINTIES.** **QUANTITATIVE: ~ 1/1,000 <P≤ 1/200**
	MODERATE	**QUALITATIVE: NOT LIKELY TO HAPPEN. CONTROLS EXIST, WITH SOME LIMITATIONS OR UNCERTAINTIES.** **QUANTITATIVE: ~ 1/10,000 <P≤ 1/1,000**
	LOW	**QUALITATIVE: NOT EXPECTED TO HAPPEN. CONTROLS HAVE MINOR LIMITATIONS OR UNCERTAINTIES.** **QUANTITATIVE: ~1/100,000 <P≤ 1/10,000**
	VERY LOW	**QUALITATIVE: EXTREMELY REMOTE POSSIBILITY THAT IT WILL HAPPEN. STRONG CONTROLS IN PLACE.** **QUANTITATIVE: ~ P≤ 1/100,000**

FIGURE 4.1-2 HAZARD LIKELIHOOD DEFINITIONS

SEVERITY	
CATASTROPHIC	PERSONNEL OR CREW: LOSS OF LIFE OR PERMANENTLY DISABLING INJURY DURING GROUND PROCESSING AT KSC, ANY PHASE OF FLIGHT (PRE-LAUNCH, LAUNCH/ASCENT, ON-ORBIT, OR ENTRY/LANDING), OR RECOVERY OPERATIONS; LOSS OF LAUNCH/FLIGHT VEHICLE OR MAJOR SYSTEM/ELEMENT DURING CREWED MISSION THAT COULD POTENTIALLY RESULT IN LOSS OF LIFE OR PERMANENTLY DISABLING INJURY. FACILITIES, EQUIPMENT, ASSETS: LOSS OF GROUND FACILITY, LOSS OF ESSENTIAL FLIGHT ELEMENT(S) (E.G., SLS BOOSTER, UPPER STAGE, CREW MODULE, PRIMARY PAYLOAD) FOLLOWING GOVERNMENT ACCEPTANCE AND PRIOR TO LAUNCH, LOSS OF LAUNCH/FLIGHT VEHICLE OR

	MAJOR SYSTEM/ELEMENT DURING UNCREWED MISSION THAT COULD POTENTIALLY RESULT IN LOSS OF PRIMARY PAYLOAD
CRITICAL	PERSONNEL OR CREW: INJURY OR OCCUPATIONAL ILLNESS REQUIRING DEFINITIVE/SPECIALTY HOSPITAL/MEDICAL TREATMENT RESULTING IN LOSS OF MISSION. FACILITIES, EQUIPMENT, ASSETS: LOSS OF MISSION, CONDITION THAT REQUIRES SAFE-HAVEN, OR MAJOR DAMAGE TO ESSENTIAL FLIGHT/GROUND ASSETS.
SEVERE	PERSONNEL OR CREW: INJURY OR OCCUPATIONAL ILLNESS REQUIRING MEDICAL TREATMENT. FACILITIES, EQUIPMENT, ASSETS: DAMAGE TO SIGNIFICANT FLIGHT/GROUND ASSETS.
MODERATE	PERSONNEL OR CREW: INJURY REQUIRING FIRST-AID TREATMENT, MODERATE CREW DISCOMFORT FACILITIES, EQUIMENT, ASSETS: DAMAGE TO NON-ESSENTIAL FLIGHT/GROUND ASSETS.
MINOR	PERSONNEL OR CREW: MINOR INJURY NOT REQUIRING FIRST-AID, MINOR CREW DISCOMFORT. FACILITIES, EQUIPMENT, ASSETS: MINOR DAMAGE TO NON-ESSENTIAL FLIGHT/GROUND ASSETS

FIGURE 4.1-3 HAZARD SEVERITY DEFINITIONS

It is important to note that ESD is developing systems for use in both crewed and un-crewed missions and that many of systems which comprise the ESD architecture will be used for both crewed and un-crewed missions. The definition of “catastrophic” in the above Figure 4.1-3 attempts to integrate these Agency definitions into an ESD Enterprise definition and these notes attempt to communicate a number of important distinctions, clarifications, and context that must be understood to properly apply of the definition of “catastrophic” within ESD.

It is common for Programs to designate certain severe, non-personnel safety scenarios as “catastrophic” due to the significant severity of their programmatic consequences. For example, with respect to facilities, equipment, and assets, the loss of vehicle or essential flight asset prior to completing its primary mission or the loss of essential ground asset may be deemed “catastrophic” by a Program or ESD in order to bring to bear the additional rigor from such a catastrophic designation. In this case, the catastrophic designation is being invoked in order to apply stricter or more clearly defined expectations for the controls and mitigations against such consequences.

The statement “**LOSS OF LAUNCH/FLIGHT VEHICLE OR MAJOR SYSTEM/ELEMENT DURING CREWED MISSION THAT COULD POTENTIALLY RESULT IN LOSS OF LIFE OR PERMANENTLY DISABLING INJURY”** in the definition of “catastrophic” is intended to convey that there are scenarios in which emergency/contingency equipment or hazard controls/mitigations may be activated or executed in an attempt to save the crew. These hazards/causes or scenarios are to be considered “catastrophic” and the mitigations are catastrophic hazard controls. Basically, when determining the severity level of the hazard or a scenario, it should be based on an assessment of the worst-case effects assuming the controls

or emergency/safing actions or hazard controls/mitigations are not in place (e.g., actions or controls may affect the likelihood component, but not the severity which is based on the potential worst-case effect). For example, SLS has a requirement to provide launch abort capability during ascent, but SLS is not allowed to take credit for this emergency capability when determining if hazard causes are catastrophic, required hazard controls, and required levels of redundancy.

A more specific example of this type of scenario would be a safing or control system recognizing a Core Stage engine redline exceedance and then taking action(s) to shut down the affected engine in order to prevent an uncontained engine failure which has the potential to result in an immediate LOC event. In this case, the safing or control system and these redlines are providing catastrophic hazard controls even if safely shutting down this Core Stage engine during ascent allows the MPCV to abort to an orbit that may be not suitable to continue the nominal mission, but allows the crew to return using nominal systems. (This example assumes that the vehicle is at a point in the mission where loss of a single engine would not impact the ability to place the MPCV in a safe orbit.) Conversely, it is also possible for failures to exist that, in the worst case, would only result in an early mission termination scenario for a crewed mission. These failures would not be catastrophic, as a worst case early termination of a crewed mission itself is not considered catastrophic.

Lastly, for non-crewed, payload missions, where the whole purpose of the mission is to place the payload in the orbit required for a successful mission, failure to do such is deemed “catastrophic” due to severe programmatic losses.

4.1.6 Non-compliances and Exceptions

4.1.6.1 Exceptions

NPR 8705.2 includes a flexible, risk-informed failure tolerance requirement which allows the Program, Technical Authorities (S&MA TA, Engineering TA, and Health and Medical TA), and Flight Crew to approve “exceptions” to the failure tolerance requirement via consensus. A lack of consensus among referenced stakeholders would initiate a dissenting opinion process as depicted in Figure 4.1.6.1-1. These “exceptions” are not considered waivers to the requirement, but instead are the allowed method for satisfying the Agency’s risk-informed approach to failure tolerance. For implementation within ESD, exceptions will be documented in the applicable hazard reports and require the concurrence of the applicable Programmatic Authority, Technical Authorities, and the Flight Crew in accordance with the risk acceptance authority identified in section 4.1.5 of this plan. For example, exceptions that result in a hazard score of 1x5 or 2x5 can be approved at either a PCB (program only hazard) or JPCB (cross programs hazard) with the concurrence of the applicable TAs and Flight Crew. At the time of baselining hazards, all failure tolerance statements should be classified as Part B or Part A exceptions except for temporary waivers as described in section 4.1.6.2. If the Program, Technical Authorities (S&MA TA, Engineering TA, and Health and Medical TA), and Flight Crew do not agree on the rationale for a part B exception, then the dissenting opinion process should be utilized as depicted in Figure 4.1.6.1-1. After baselining of the hazard analysis, if there is a change to a previously

agreed to part b exception that results in an increase in risk then the waiver process outlined in section 4.1.6.2 should be utilized.

Appendix F in this document contains classes of hazard causes that are pre-determined to be excepted from the failure tolerance requirement. These classes cover causes such as “Improper or inadequate definition of environments,” “Improper system configuration,” etc. The table also contains the generic controls for these classes of causes.

Per Chief OSMA, each CSO will provide a list of proposed failure tolerance exceptions per guidance in Figure 4.1.6.1-1. The Chief OSMA will review the list and determine which items (if any) are to be discussed in more detail.

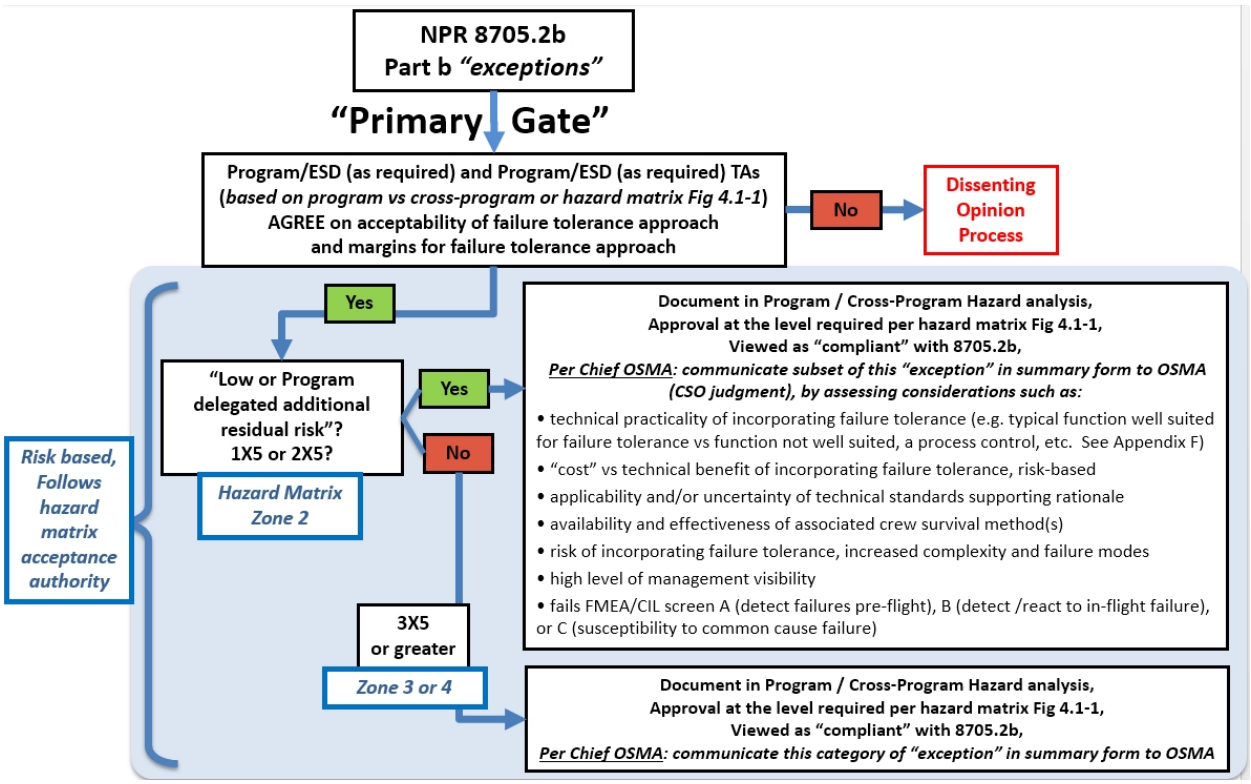


FIGURE 4.1.6.1-1 PART B EXCEPTION PROCESS

4.1.6.2 Waivers

Proposed waivers to the Human Rating requirements as stated in NPR 8705.2, require the concurrence of the requesting Program Manager/ESD Director and Program/ESD CSO, Program/ESD Chief Engineer, Health and Medical TA, and Crew Office. These waivers will be included in the Human-Rating Certification Package (HRCP).

The following would define the need for a waiver against specifically the failure tolerance requirement (ref. NPR 8705.2, sections 3.2.3.b). First, if a change is requested after formal hazard report baseline to a previously agreed-to “part b exception” failure tolerance strategy, and if the change creates an increase in risk acceptance, then a waiver would be required. Unlike “part b exceptions” which are allowances documented within hazard analysis, the waiver would be a separate standalone configuration controlled document. Second, if a “part b exception” failure tolerance strategy requests the acceptance of an elevated level of risk for a temporary period of time or numbers of flights, then a waiver would be required to cover the temporary period of time or number of flights of elevated risk acceptance due to the temporary failure tolerance strategy. Waivers should be brought forward as soon as the conditions above are known and met.

The following would define the need for a waiver against the exceptions to the failure tolerance requirement for failure of primary structure, structural failure of pressure vessel walls, and structural failure of pressurized lines (ref. NPR 8705.2, section 3.2.3.a). The process for “part a exceptions” is similar to that for “part b exceptions”. First, if a change is requested after formal hazard report baseline to a previously agreed-to “part a exception” and if the change creates an increase in risk acceptance, then a waiver would be required. Second, if a “part a exception” requests the acceptance of an elevated level of risk for a temporary period of time or numbers of flights, then a waiver would be required to cover the temporary period of time or number of flights of elevated risk acceptance due to the temporary hazard control strategy. Again, waivers should be brought forward as soon as the conditions above are known and met.

4.1.7 Analysis of Program Change

All Program and ESD change requests will be assessed for impact to the hazard analysis as part of the program’s change evaluation process. This is to assure that potential hazards or hazard causes are not introduced or controls weakened without program approval. As part of the change package, an impact to baselined hazard causes will be identified along with acceptance rationale. Any potential increases or decreases in the baselined cause risk will be identified. A change will be considered to involve an increase in baselined risk if any of the following is true:

a. The change introduces a new hazard or new cause(s).
b. The change eliminates or adversely affects previously defined hazard controls or hazard control verifications.

c. The change increases probability of a hazard or critical failure mode manifesting itself. This could include supporting probabilistic risk analysis, where reasonable and available, in order to provide an assessment of impact on Loss Of Crew (LOC) risk.

d. The change increases the severity of a previously identified hazard, hazard cause, failure mode, or failure cause.

4.1.8 Cross Program Integrated Hazard Analysis Inter-Relationship with FMEA/CIL

The safety hazard analysis and FMEA/CIL are complementary analyses that by themselves have unique limitations, but together provide a comprehensive means to identify, understand, and eliminate or control the safety and reliability risks present in the design and intended operations. Proper coordination between these analyses is important to reduce duplication and ensure their maximum effectiveness.

The FMEA/CIL will provide data to support the hazard analysis in the assessment of compliance with failure tolerance requirements, and the identification, control and/or verification of hazard causes. Hazard analyses will provide appropriate references to applicable FMEA/CILs or sections thereof. At the discretion of the hardware developer, controls and verifications for hardware failure modes may be documented either directly in the applicable hazard products or through linkage to specific CIL retention rationale.

4.1.9 Cross Program Integrated Hazard Analysis Inter-Relationship with the Cross Program Integrated Probabilistic Risk Assessment (IPRA)

Previous programs have experienced inconsistencies between S&MA products and have proposed lessons learned to help bridge those gaps. One such gap is between hazard analyses and PRA. Hazard analyses help identify the initiating events that a PRA assesses with Event Sequence Diagrams and event trees developed to a specific end state, and then quantifies the likelihood of that scenario. The hazard analyses also assess the likelihood of each hazard cause. Therefore, to minimize gaps, the two S&MA disciplines will work together to produce a more consistent set of S&MA products. The XPRAT team members will be part of the cause tree development. The interim products from each team will be compared to identify inconsistencies or gaps between the products. The IHAITT and XPRAT will collectively address any inconsistencies that may require updates to the analyses to properly document the risks. Where hazards have the potential for significant risk, the XPRAT will work with program and integrated hazard developers to provide likelihood levels for selected hazard causes, consistent with the Cross Program IPRA. The two teams will continue to share data through sharing and reviewing each other's maturing analyses.

4.1.10 Crew Survival Analysis

Per NPR 8705.2B, Human-Rating Requirements for Space Systems, ESD programs will describe the crew survival strategies through all phases of the reference mission. The descriptions will include identification of the system capabilities required for the crew survival methods. ESD programs are not required to provide a crew survival capability for all failure scenarios, but are expected to provide survival capabilities to the extent practical within other constraints on the program (e.g. cost, schedule, performance, risk).

As with all aspects of human rating, crew survival must be addressed as an integrated space system. Therefore, ESD programs will collaborate to produce MPCV 72532, Orion Multi-Purpose Crew Vehicle (MPCV) Program Crew Survival Analysis for the EM-2 Reference Mission at major milestones and as a deliverable to support the Human-Rating Certification Package. The Orion MPCV Program will lead the development of the CSAR.

Crew survival requirements in NPR 8705.2B were analyzed by the Cross program Human Rating Team to determine requirements for each ESD program. Each ESD program will incorporate these responsibilities into program requirement documents, or elevate disagreements to the Joint Program Control Board (JPCB) for resolution.

Hazard cause developer will assess each program hazard and Cross Program integrated hazard cause, for available crew survival methods should all hazard controls fail and the hazardous condition occur. Initially, prior to PDR, all potential survival methods will be inventoried and assessed by the crew survival analysis team, with qualitative descriptions of effectiveness and likelihood of success. At each successive review of the hazard products, crew survival methods will be reassessed for validity, level of implementation and verification in the program(s), and updated characterization of effectiveness and likelihood of success. Where possible and reasonable, the effectiveness and likelihood of success will be quantified. (Note: Aborts and other crew survival methods are not considered as hazard controls).

The CSAR compiles all crew survival methods and identifies applicability across the mission phases. The crew survival capabilities are reviewed and included also in the LOC IPRA as applicable. Crew survival analysts determine if there are any gaps in crew survival coverage (i.e. hazards without a survival method), or where the survival capabilities have a low likelihood of success. The results of the crew survival analysis are briefed to applicable program systems engineering forums in a timely fashion to permit program mitigation of gaps or risks as much as possible.

The CSAR is approved via cross program change request. At each Program milestone review, the program will address compliance with required crew survival capabilities. The CSAR is delivered as part of the Human Rating Certification Package (ESD 10009). Content and maturity criteria for the Cross program Crew Survival Analysis Report can be found in Appendix E.

4.1.11 CSAR Inter-Relationship with FMEA/CIL

The CSAR and FMEA/CIL are complementary analyses that by themselves have unique limitations, due to the CSAR being a top-down assessment and the FMEA/CIL being a bottoms-up assessment, but together provide a comprehensive means to identify, understand, and eliminate or control the safety and reliability risks present in the design and intended operations of the Crew Survival Systems during emergency situations. Proper coordination between these analyses is important to ensure their maximum effectiveness.

The FMEA/CIL data can be used to support the CSAR in the assessment of failure tolerance associated with the usage of crew survival systems during emergency situations and can be used to aid in identifying, controlling, and verifying the capabilities of the emergency systems.

4.2 GROUND PROCESSING SAFETY

Each program will address ground processing safety and hazard analysis requirements as part of its Program S&MA Plan for operations, including work performed at KSC in an Industrial Operation Zone (IOZ) area prior to turnover to GSDO.

Orion MPCV and SLS will support ground processing hazard analysis development activities by providing data and/or analyses for pre-flight activities associated with the respective Program system.

For work performed in an IOZ area at KSC, the respective programs will deliver hazard analyses and supporting data, for critical and catastrophic hazards, which could propagate outside of the IOZ, to GSDO for review and incorporation into GSDO safety and operations products as needed.

Ground safety requirements for post-turnover flight hardware processing can involve either the flight hardware design or represent operational tasks related to hazard controls. Ground safety requirements that are based on the flight hardware design (e.g., a propulsion system having mechanical inhibits against bulk propellant leakage) will be established in ICDs and/or IRDs or other appropriate cross program requirements documentation. Ground safety requirements that represent operational tasks (e.g., a requirement for GSDO to perform a joint leak check after Booster stacking) will be established in the Cross program Operations and Maintenance Requirements and Specification (OMRS) or Work Authorization Documents (WADs).

GSDO will lead and develop a Program-Only ground processing hazard analysis (which will integrate the inputs from SLS and Orion MPCV) to address hazards and hazard mitigation strategies for all ground processing hazards beginning with hardware turnover to GSDO until the start of cryogenic loading prior to launch.

From the beginning of cryogenic loading until the beginning of post-flight recovery operations (after crew egress), the CPIHA will identify and document the cross program (integrated) hazard causes per Section 4.1.2.3 of this plan. Formal risk acceptance of these cross program (integrated) hazard causes will be per Section 4.1.6 of this plan.

It should be noted that to ensure identification and documentation of GSDO Program-Only hazards and mitigation strategies associated with ground processing operations, the GSDO Program-Only ground processing hazard analysis will also analyze the processing timeframes of cryogenic loading until the space system clears the launch tower on ascent, post-flight recovery operations, transportation of the recovered Crew Module (CM) back to KSC, and CM de-servicing at KSC until hardware disposal or turnover to the appropriate program or contractor. This may include identification of some hazards (e.g., premature umbilical separation, failure of an umbilical to separate, umbilical re-contact with the launch vehicle) that meet the criteria of a cross program (integrated) hazard cause, which represents a slight overlap with the set of CPIHA integrated hazard causes. In these instances, the GSDO Program-Only hazard cause will “point” to the appropriate CPIHA integrated hazard cause record(s), which contain the entire set of controls for the integrated hazard cause.

Ground systems (Ground Support Equipment (GSE) and Government Furnished Equipment (GFE) delivered to the GSDO Program) that are owned by SLS or Orion MPCV, and used during ground processing including recovery operations, will have the hazard analysis performed by the owning Program. Orion MPCV and SLS will deliver the hazard analysis and supporting data for critical and catastrophic hazards to GSDO as source data for incorporation into GSDO safety and operations products (e.g. GSDO Program-Only hazards), and residual risk acceptance by GSDO, as needed. For use as-is Heritage GSE, the GSDO Program will follow GSDO-PLN-1002, GSDO Systems Engineering Management Plan (SEMP) for determination of appropriate analyses.

The GSDO Program S&MA Plan will address the methodology for the ground processing hazard analysis and the process for acceptance of residual ground safety risks, including risks to the SLS and Orion systems.

4.3 RANGE SAFETY

ESD programs are required to comply with tailored Air Force Space Command Manual, 91-710 and NPR 8715.5, NASA Range Safety Requirements. The tailored requirements are located in the following documents: ESD-10114-01, ESD-10114-02, ESD-10114-03, ESD-10114-04, ESD-10114-05, ESD-10114-06, ESD-10114-07, and ESD-10114-08.

ESD has chartered the Human Exploration Range Safety Panel (HERSP) to integrate and define the approach for ascent and entry range safety, including negotiation of requirements and deliveries with the Air Force Range Safety offices. Refer to the HERSP Task Agreement for more details.

HERSP Task Agreement:
http://nasa-ice.nasa.gov/confluence/display/HERSP/Range+Safety+Task+Agreement

4.4 PAYLOAD SAFETY

For EM-1, each program will develop a consistent secondary payload safety process and payload safety requirements applicable to their program. Secondary payload cross program integrated hazards will be approved at the cross program integrated hazard level consistent with this document and ESD 10015.

4.4.1 Safety Review Process <TBD-10010-011>

4.5 INDUSTRIAL SAFETY

NASA Centers and contractors are required to comply with federal, state, and local safety regulations. NASA industrial safety requirements do apply to NASA Centers and each Center

establishes local policies and procedures, which comply with NASA requirements as well as state and local regulations. NASA contractors are required to comply with NASA Center requirements for all activities on a NASA Center (except in Industrial Operations Zones (IOZs). NASA industrial safety requirements do not apply to NASA contractor operations located off NASA sites.

4.6 MISHAP PREPAREDNESS AND CONTINGENCY PLAN

Each ESD program is required to have a Mishap Preparedness and Contingency Plan (MPCP) for stand-alone operations that comply with NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping. Program MPCPs are identified in section 2.2.

For integrated ground operations and flight operations, the ESD MPCP takes precedence and serves as the integrated plan.

4.7 ORBITAL DEBRIS ASSESSMENT

Orbital Debris Assessment Reports (ODARs) will be submitted for Orion MPCV and SLS in accordance with NPR 8715.6A, NASA Procedural Requirements for Limiting Orbital Debris and NASA-STD-8719.14A, Process for Limiting Orbital Debris, to determine the potential for orbital debris generation.

NPR 8715.6A provides the requirements to implement NASA's policy for limiting orbital debris generation per the U.S. National Space Policy, the U.S. Government Orbital Debris Mitigation Standard Practices, and as a part of NASA's policy for safety and mission assurance programs as defined in NASA Policy Directive (NPD) 8700.1. Any non-compliance to orbital debris requirements, including those for reasons of mission requirements and cost effectiveness, require a variance to this NPR.

NASA-STD-8719.14A serves as a companion to the NPR 8715.6A and provides specific requirements and methods to comply with the NASA requirements for limiting orbital debris generation. The standard helps ensure that spacecraft and launch vehicles meet acceptable standards for limiting orbital debris generation.

The standard establishes requirements for (1) limiting the generation of orbital debris, (2) assessing the risk of collision with existing space debris, (3) assessing the potential of space structures to impact the surface of the Earth, and (4) assessing and limiting the risk associated with the end of mission (EOM) of a space object. Additionally, the standard provides the format for the required debris assessment (ODAR), which must be submitted to the Office of Safety and Mission Assurance as required in NPR 8715.6A.

These required ODARs must address the potential for orbital debris generation that results from normal operations and malfunction conditions, and on-orbit collisions. These can further be categorized into the following seven issues to assess:

- Debris released during normal operations;

- Debris generated by explosions and intentional breakups;
- Debris generated by on-orbit collisions during mission operations;
- Reliable disposal of spacecraft and launch vehicle orbital stages after mission completion;
- Structural components impacting the Earth following post-mission disposal by atmospheric reentry;
- Disposal of spacecraft and launch vehicle stages in orbits about the Moon; and
- Debris generated by on-orbit collisions with a tether system.

The nominal ODAR delivery schedule for each program is as follows, where the referenced milestones are those specific to each program.

- PDR ODAR – Delivered at the Preliminary Design Review (PDR)
- CDR ODAR – Delivered 45 days prior to the Critical Design Review (CDR)

The Final ODAR is submitted 30 days prior to the Safety and Mission Success Review (SMSR) as a part of the launch approval process. This ODAR will be a single integrated package that contains the Final ODARs for each program. Orion MPCV Safety and Mission Assurance will be responsible for integrating the Final ODAR and submitting if for review and approval.

5.0 RELIABILITY AND FAILURE MODES

5.1 FMEA/CIL INTEGRATION TASK TEAM

A cross program Failure Mode & Effects Analysis/Critical Items List (FMEA/CIL) Integration Task Team (ITT) has been established under the System Safety Functional Area. FMEA/CIL ITT primary objectives are to (1) identify failure modes of each Program that can affect other Programs and their cross Program effects, (2) confirm that the criticality designation for Programs on either side of each interface is correct and consistent, and (3) determine the appropriate cross program critical item controls and verifications, and (4) work towards a resolution of any discrepancies and their potential programmatic (schedule, budget, contracts, etc.) and/or design impacts.

Each Program will establish requirements and methodology for development and maintenance of the Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL). The scope of each Program's FMEA/CIL will include flight hardware and flight critical Ground Support Equipment (GSE). Flight critical GSE is defined as GSE that physically or functionally interfaces with flight hardware during the integrated timeline (cryo loading to post-flight crew egress) that can cause a critical or catastrophic hazard. As part of producing the Program FMEA/CIL, each Program is responsible for identifying failure effects that may cross Program boundaries and affect another Program. In these cases, the FMEA/CIL ITT will facilitate exchange of information between Programs to assure that there is a clear understanding of the integrated failure effects. The FMEA/CIL ITT will utilize a FMEA interface matrix as an assurance tool for assessment of the Program-to-Program interfaces. Representatives from each affected Program will

collaborate through technical interchange meetings to review the integrated failure effects, confirm the accuracy and completeness of the affected Program FMEAs, determine mitigation strategies and retention rationale (where appropriate), agree on documentation responsibilities, and agree on CIL verification requirements. Results of these reviews will be recorded in the FMEA interface matrix. Additional information regarding the purpose and content of the FMEA interface matrix and a summary of identified cross program FMEA issues can be found in ESD 20001, “Cross Program FMEA Integration Summary Report”.

The FMEA/CIL ITT will archive and share Program FMEA/CILs among all Programs. Program FMEAs and CILs will be approved at the responsible Program’s appropriate control board (e.g. PCB), with representation from the other affected Programs, as appropriate. CIL design, test, and inspection controls, which are imposed on another Program, will be documented in ICDs or IRDs for needed design changes, or other bilaterally agreed upon processes such as OMRS. Verification of these imposed CIL controls is the responsibility of the performing Program.

The FMEA/CIL ITT lead will provide status of the FMEA/CIL integration activities to the CPIT FAL on a regular basis. In the event that the Program FMEA leads are not able to reach consensus on FMEA/CIL issues affecting multiple Programs, the issue will be elevated by the System Safety FAL to the CPIT for resolution.

5.2 COMMON FMEA CONTENT

Use of a common FMEA/CIL methodology by all Programs is not required; however, some data fields and definitions need to be common to allow for proper integration.

5.2.1 Common Criticality Definitions

To ensure consistency of FMEA/CIL analysis among the Programs, the following definitions for criticality are established. These definitions may be tailored by each Program to address Program-unique needs so long as the intent is not significantly altered and ESD and Program CSOs concur. To obtain CSO consensus, the FMEA ITT will discuss and present proposed tailoring at a CSO tag-up. The consensus decision will be documented in the CSO minutes.

TABLE 5.2-1 CRITICALITY CATEGORY DEFINITIONS

Criticality	Definition
1	Single failure that could result in loss of life or vehicle
1R#	Redundant hardware that, if all failed, would result in loss of life or vehicle. A number (#) is used to indicate the number of failures that must occur before the criticality 1 effect is manifested
1S	Single failure of a safety or hazard monitoring hardware item that could cause the system to fail to detect, combat, or operate when needed during a hazardous condition, potentially resulting in loss of life or vehicle.
2	Single failure that could result in a loss of mission

2R	Redundant hardware item that, if all failed, could cause loss of mission
3	All other failures

5.2.2 Failure Effect Levels

For each failure mode, the Program FMEAs will describe the worst-case credible failure effects. The failure effect descriptions must be sufficiently detailed to clearly describe impacts on item/element/vehicle required functionality and interfaces. For redundant systems, the analysis will address the loss of all redundancy. The failure effects will be described at the following indenture levels:

a. Immediate Effect – Failure effect on the item under analysis, the assembly it is associated with (if appropriate), and its interfaces.

b. Next Effect – Failure effect at the next higher assembly level, typically the subsystem/system, and ultimately at the SLS/Orion /GSDO element level

c. End Effect – Failure effect at the integrated vehicle level, including effects on the Orion/payload, mission, and crew

5.2.3 Interfaces

Each Program's FMEA will include assessment of system/subsystem interfaces within the element, between elements, and with the interfacing Programs. The analysis of a component whose failure may propagate across an interface will not end at the interface with other elements/systems/programs, but must be communicated to the impacted entities and analyzed across the interface to determine effects on the interfacing element and ultimately on the vehicle, Orion/payload, crew, and mission.

5.3 SYSTEM RELIABILITY PREDICTIONS

Reliability predictions for flight hardware and flight critical GSE are developed and controlled by each Program as described in their respective Program S&MA Plans. Reliability engineering representatives share reliability prediction data across the Programs to ensure the most appropriate reliability data is available and used in each Program. Each Program supplies reliability estimates (i.e., failure rates) for use in launch availability analyses, probabilistic risk assessments, system trade studies, and other purposes as required.

6.0 QUALITY ASSURANCE

6.1 PROBLEM REPORTING AND DISPOSITION

6.1.1 Non-conformances

Each program will establish non-conformance reporting systems for its pre-DD250, pre-turnover operations and document such approach in its Program S&MA Plan.

During post-turnover operations to GSDO, non-conformances with SLS or Orion hardware/software detected by GSDO will initially be entered into the GSDO non-conformance system. The GSDO system will be used to document the discrepancy, its resolution, as well as the remedial action and verification of preventive/recurrence control actions. Post turnover, GSDO will make non-conformances visible to both Orion MPCV and SLS in the Cross Program Problem Reporting and Corrective Action (CP PRACA).

6.1.2 Integrated Material Review Boards

GSDO will coordinate the disposition and final closure of any non-conformances with the appropriate Program. Disposition and final closure will need the required signatures as detailed in each Program SMA requirements. The process will be defined in Appendix G of this plan. Until the required representatives from the Program approve the disposition, the design attributes of the nonconforming material will not be further processed. Material Review Board (MRB) final summary containing the technical and flight safety rationale require formal concurrence from the appropriate Program.

6.1.3 Cross Program Reportable Issues and Anomalies

Pre-turnover to GSDO, significant Orion MPCV and SLS non-conformances, issues and anomalies (e.g. Crit 1/1R functional failures) that meet the elevation criteria defined in their program S&MA requirements are to be made available electronically via CP PRACA. Post-turnover, KSC will make all Orion MPCV and SLS non-conformances available to all stakeholders in CP PRACA.

6.2 DATA REQUIREMENTS FOR HARDWARE HAND-OVER

When contractually required by the procuring agency, Acceptance Data Packages (ADP's) for flight hardware/material, GSE, and ground hardware will be made available to GSDO. Where GSDO will be performing sustaining engineering activities, ADP's will be turned over to GSDO for configuration control. Content and format will be determined by the procuring agency, as provided in their respective S&MA Plans.

The flight hardware ADP data requirements for Orion MPCV and SLS are defined in MPCV 70146, MPCV ADP Requirements, and SLS-RQMT-014, SLS S&MA Requirements respectively. The flight hardware ADP requirements for GSDO are defined in GSDO-PLN-1143, Cross program Flight Hardware/Software ADP Plan. For GSE and ground hardware that is turned over to or used by GSDO as negotiated between programs, the Cross Program ADP data requirements are defined in GSDO-PLN-1027, Cross Program Ground Hardware/Software Acceptance Data Package. This data may be provided as part of an ADP or as a separate data request by GSDO. For all Rotational equipment, End User Reference Data minimum content guidelines can be found in GSDO-PLN-1055.

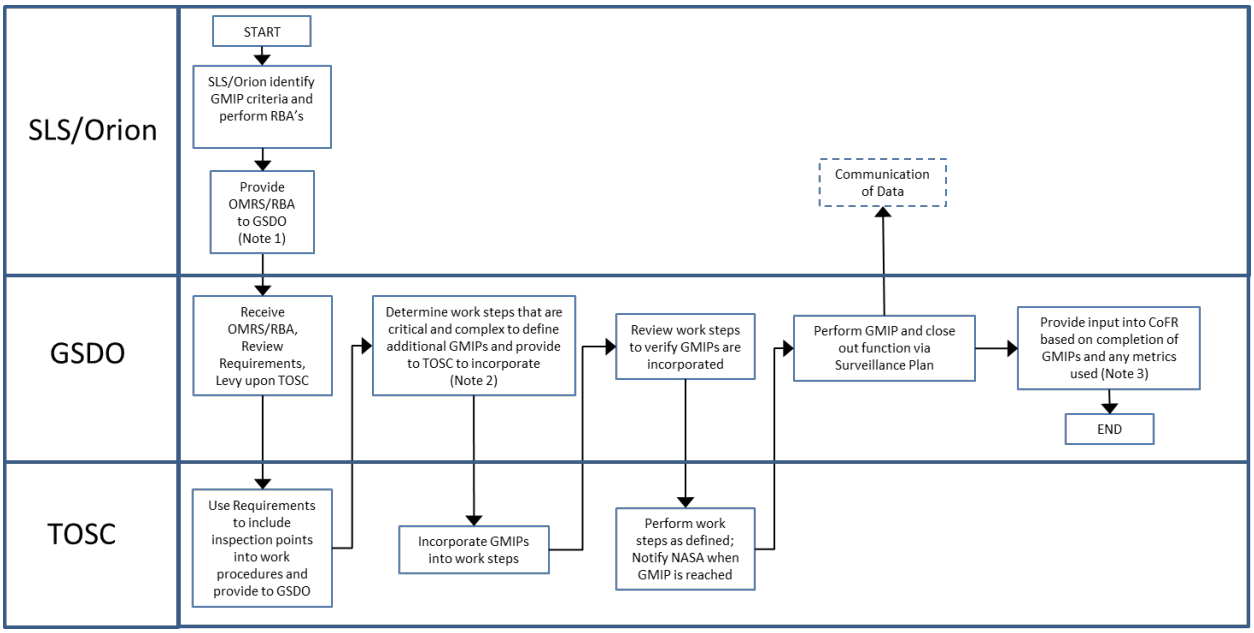
6.3 SUPPLIER AUDITS

Each program will conduct audits of supplier policies, procedures, and operations which implement the quality program. These audit processes will be documented in their Program S&MA Plan. Where multiple programs need to audit a single supplier for multiple contracts, the

programs will coordinate and integrate audit efforts to minimize the burden on the supplier. The Quality Integrated Task Team (QuITT) will ensure that the proper supplier audit coordination is accomplished. For audits of sub-tier suppliers, each Program will accompany their Prime Contractors as applicable. These audits will be documented in that contractor's system.

6.4 GOVERNMENT MANDATORY INSPECTION POINTS (GMIPS)

Each program will establish GMIP criteria and processes for its pre-DD250, pre-turnover operations and document the approach in its Program S&MA Plan. Post-turnover, SLS and Orion MPCV will identify the types of operations that require GMIP's along with inspection or verification activity criteria, as well as any Risk Based Assessments (RBA's) for processes that require surveillance. GSDO will establish an approach for GMIPs for ground hardware processing and integration and will implement SLS/Orion MPCV requirements. See Figure 6.4-1.



Note 1: OMRS will include design requirements criteria based on hazards, FMEA/CILs and RBA that will determine inspections (Contractor/Government).
Also forward work can include open inspections (contractor/government) which will be transferred to GSDO to implement. Completion of these can be fed back to originating program if needed, but will be controlled by GSDO.

Note 2: This will be part of the surveillance planning process. GMIPs definition is based on NPR 8735.2, but other surveillance techniques can be performed for "high risk" items.

Note3: Any forward work inspections (contractor/government) that were performed could be communicated back to the originating program.

General Note: Any nonstandard work stemming from non-conformance dispositions will include GMIPs as required

FIGURE 6.4-1 CROSS PROGRAM – GMIP PROCESS

6.5 QUALITY INTEGRATED TASK TEAM

The QuITT is a Cross Program forum to facilitate quality assurance issues and concerns across the Programs/Elements. In particular, sharing of quality assurance information that could potentially affect other Programs, Elements, or the integrated vehicle should be brought for discussion.

The QuITT will identify cross program issues and information that are candidates for elevation to integrated management forums within ESD. Such candidates may include trends in significant non-conformances or quality issues (e.g. process escapes), cross program quality initiatives, etc. For each candidate, an assessment of likelihood and severity will be performed. Those items that are assessed with significant risk will be carried forward to ESD for discussion. The QuITT will coordinate these items with ESD prior to elevation. Each program will document its approach to communicating quality topics to program management in its Program S&MA Plan.

7.0 ESD PROBABILISTIC RISK ASSESSMENT

7.1.1 Cross Program Probabilistic Risk Assessment (XPRA)

7.1.1.1 Objectives

XPRA has three specific objectives to facilitate risk-informed decisions by ESD during the design, development, and operation phases:

a. **Quantitative Risk Requirements Establishment**: Establishing quantitative risk requirements, or removing the “To Be Resolved” designations, is performed using analysis early in the program life cycle and again as the design matures. NASA’s preferred approach to this process is PRA, as specified in Agency NASA Procedural Requirements (NPRs) and standards. The PRA should be supplemented with available deterministic analyses and other data to make it a best-estimate of achievable risk levels for a given reference mission.

b. **Quantitative Risk-Informed Design Trade Studies**: Quantitative risk informed design trade studies use the “current” PRA of the vehicle and/or mission to assess design options offered as a means of reducing risk or assessing the risk impact of improving other performance measures. The “current” PRA is a product of a “living PRA” approach that is maintained and updated throughout the program’s life cycle. It would be the best-estimate risk assessment at any point in time. The PRA must be supplemented with current and relevant deterministic analyses and other data to make it a legitimate trade study.

c. **Quantitative Risk Requirements Verification**: Verification of quantitative risk requirements is also performed using analysis. NASA’s preferred approach to this verification is PRA, as specified in Agency NPRs and standards. The PRA must be supplemented with deterministic analyses and other data to make it a legitimate assessment.

7.1.1.2 Integration

The complex and interactive nature of NASA's exploration architectures requires an integrated effort in order to understand the interaction of systems and to account for failure scenarios initiated in one mission phase that manifest in later phases. Two very notable examples are ascent aborts and debris strikes to re-entry Thermal Protection System (TPS).

Stand-alone probabilistic models by themselves are insufficient for capturing and quantifying the effects of integrated system interactions. The overall model design should allow for integration, much like the elements themselves are eventually integrated into a functioning space system. This requires that all sides involved collaborate in the planning of the integrated model structure, the definition of the interfaces between models, and the assignment of responsibilities and associated timelines for building the pieces of the model.

The Cross Program PRA Team (XPRAT) was formed to provide a forum for PRA representatives from each program to collaborate to fulfill the ESD PRA objectives. In addition, the XPRAT will:

a. Develop, establish, and maintain the standard methodology by which the SLS, MPCV, and GSDO programs will perform an integrated, consistent PRA for the Cross Program (XP). This ESD 10011, Cross Program Probabilistic Risk Assessment Methodology document will be shared across the XPRAT.

b. Establish a Cross Program working group to build, maintain, and apply the integrated PRA. This includes documentation of the Cross Program PRA at all levels to capture the system description, assumptions, data analysis, engineering inputs, and results in order to preserve the basis of the analysis for internal and external peer reviews.

c. Identify and incorporate partnership considerations and opportunities between outside organizations, such as the crew office, mission operations, engineering, and human health and performance.

d. Perform architecture risk analysis and key trade studies across all elements, including DRMs, manifests, launch campaigns, and phased development plans.

e. Establish, maintain, and report technical performance measures in response to ESD reporting requirements for quantitative risk. This will be done through coordination with the program PRA team members, the ESD and program CSOs, and reported on an agreed upon frequency.

f. Provide and maintain schedules including points at which the integrated model will be drafted and updated in support of integrated milestones and Human Rating Certification Package (HRCP) delivery/endorsement.

g. Identify primary interface points between system models and integrated models among the XPRAT.

h. Recommend quantitative risk requirement values, Technical Performance Measurements (TPMs) and mission phases allocations for ESD and program-level requirements documents.

i. Document roles and responsibilities for all organizations involved in building and maintaining the integrated PRA.

j. Support the Agency in the development of loss of crew thresholds and goals.

7.1.2 Requirements

Quantitative risk requirements are defined in ESD 10002, Explorations Systems Development (ESD) Requirements. The Level 1 risk requirements are expected to be imposed for specific DRMs as the mission Concepts of Operation (ConOps) are developed. The SLS, MPCV, and GSDO programs will collaborate in further allocation, flow down, analysis, and verification of the LOC requirements as needed.

Using agreed upon methodologies and data, the XPRAT will develop a preliminary PRA of each DRM and determine appropriate risk allocations for each ESD program in order to achieve the Level 1 requirements. If the program agrees with the allocation, the program will formalize the allocation as a requirement in its System Requirements Document, or equivalent program specification. If there is disagreement over allocations, the issue can be elevated through program and ESD management forums in accordance with ESD 10001, ESD Implementation Plan.

ESD actively manages both expectations/requirements and their corresponding compliance metrics for Loss of Crew (LOC), a likelihood distribution calculated using Probabilistic Risk Assessment (PRA) techniques. The flow of LOC management can be seen first at the highest level within the Agency with the establishment of specific LOC thresholds and longer-term goals for either a class of or a specific DRM. The approach defines the ultimate Agency-level (NASA Administrator-level) LOC risk tolerance for either a class of or a specific DRM, and is then used as a communication and management tool both down-and-in as well as external to the Agency. ESD then creates/manages ESD-level LOC requirements and/or performance metrics to assure development of ESD systems are compliant with overarching Agency-level LOC threshold (and with margin). Furthermore, MPCV and SLS have their own program-level LOC “sub allocation”, which allows each program to have a clear design requirement to measure against at the program-level. It is important to note, however, that each program having an LOC “sub-allocation” does not equate to each program’s LOC landscape being a separate/individual stovepipe, as significant cross program interplay can exist with respect to LOC assessment per mission phase. For example, significant SLS ascent failures/risks (likelihood and consequences) establish initial conditions for MPCV ascent abort scenarios; thereby crossing program boundaries and driving overall ascent phase LOC. At each HRCP endorsement milestone and ESD milestone review, LOC assessment snapshots are completed at all levels to compare current LOC assessments against thresholds/requirement/metrics at all levels. These milestones are also an opportunity to re-evaluate the LOC thresholds/requirements/metrics themselves.

To integrate PRAs performed by multiple, geographically dispersed organizations, some degree of commonality of approach is required to assure that such PRAs can indeed be integrated and provide confidence in using the results as a decision making aid. As with any other resource (e.g., money), balancing risk across multiple systems can be hampered without a common accounting methodology and could even result in making the wrong decision if program methodologies are too disparate. ESD programs will provide PRA models and data which comply with ESD 10011 Cross Program Probabilistic Risk Assessment Methodology.

The XPRAT will report status of analysis progress and requirement compliance to the Cross Program Integration Team (CPIT) and higher forums as required. Prior to reporting the results, the XPRAT will review those results of the Integrated PRA to ensure that the risk drivers, methodology, and data are credible. Once it has been determined that the model and data are acceptable, the XPRAT may assign actions to its program representatives to report and discuss the results of the analysis with their program prior to presenting the results outside of the XPRAT. The XPRAT will then bring the results forward to the Joint Integration Control Board (JICB). The PRA results may require further communication to higher-level ESD forums, particularly if there are technical issues that require ESD decisions or deficiencies indicating potential non-compliances with ESD risk requirements. The JICB will determine the forward reporting path following the governance structure described in ESD 10001, ESD Implementation Plan.

7.1.3 Risk-Informed Design

Each program is required to establish a systems engineering process which considers safety, reliability, and risk in system design processes. Each program defines this process in their respective program documentation.

The Cross Program PRA also needs to inform the program system engineering process. The Cross PRA will be compiled from program inputs, and results of the integrated PRA will be shared with the program representatives on a continual basis informally to help inform the programs of risk drivers and Level 1 risk requirements compliance status. For risk drivers that are wholly caused and controlled by a single program, the XPRAT will expect that the owning program will address those risk drivers internally for mitigation/reduction as needed to meet their risk allocations. For risk drivers that are truly integrated in nature (i.e. require actions from multiple programs to mitigate), then such risk drivers will be discussed with the JICB with recommendations for risk mitigation or acceptance. The JICB will elevate issues and recommendations for visibility or decision as needed.

If a program is within allocation, and the Cross Program PRA indicates compliance with Level 1 requirements, then residual risk for that program can be proposed for acceptance by the ESDCB. However, even when compliance is achieved, NASA policy requires that ESD programs pursue continuing efforts to further reduce risks by on-going financial investments in technology development, testing, and new design. Each ESD program will define a strategy for continuous risk improvement as part of their respective program documentation.

The most critical aspect of informing the design is the timing that allows PRA results to be a part of design decisions at the time they are being made. Again, consistency between IHA Cross Program Hazard Analysis and XPRA will help during these discussions. Building a PRA requires

design input for the PRA models to be constructed. The systems engineering process must take this into account by incorporating iterative analysis cycles to assess design concepts for safety, reliability, and risk, while optimizing the design against all performance parameters until the design trades have resulted in an optimum balance of risk, performance, cost, and schedule that can be accepted by the program stakeholders. Clearly, Cross Program PRA results will lag program analysis and design efforts, which presents some risk that XPRA results will not be timely inputs for program-level decisions. However, the majority of XPRA risk drivers will be unique to a single program and program-level analysis will identify those and work them to resolution. The number of integrated risks requiring multi-program actions to mitigate will be somewhat limited and are identified in advance by the XPRAT and are areas of high focus to address early. The XPRAT will participate in aborts planning and other working teams to address these integrated risks so that PRA results can help inform and focus the team. With the XPRAT focused on these integrated risks, and the programs focused on uniquely-owned risks, the PRA efforts can inform the design activities in a reasonable time. Agreements reached between programs on multi-program risk mitigation strategies that require new changes to the design will be documented in the appropriate ICDs and IRDs.

In the program phases prior to verification closure, there will be points at which the integrated model will need to be formally updated. The XPRA will be updated prior to ESD integrated milestone reviews and also for each major milestone where the HRCP is endorsed. However, for PRA to be an effective design and decision-making aid, informal or preliminary results will be sought at points between planned updates. Any PRA model, integrated or not, should have a quick-response capability that supports decisions at any time during the life cycle. All parties building pieces of the Cross Program PRA must be aware of this and embrace model designs that facilitate quick-turnaround estimates, even if they are rough order of magnitude.

7.1.4 Products and Quality Assurance

MPCV is responsible for the generation of XPRAT products and maintaining the supporting data. SLS and GSDO are responsible for providing specific inputs to those products, review and concurrence of XPRAT products, and supporting the presentation of XPRAT products to external parties to help explain their program content.

MPCV will generate the Cross Program PRA model in accordance with ESD 10011 Cross Program Probabilistic Risk Assessment Methodology, and retaining all supporting analysis, reliability, and design data necessary to establish verification of the Level 1 risk requirements.

SLS and MPCV are responsible for providing models, data, and supporting information in accordance with data exchange requirements as necessary to produce the Cross Program PRA (XPRA). GSDO is responsible for only providing data and supporting information in accordance with data exchange requirements as necessary to produce the XPRA. XPRAT will develop GSDO models, as needed, with GSDO support. Each program will also be responsible for defending the basis of calculated risks from that program. XPRAT is responsible for coordinating the integration of the program PRAs to produce the XPRA as well as assessing relevant human reliability probabilities and adding the appropriate medical risk from the integrated medical model. Programs are responsible for the quality assurance of their products

and information, as well as responding to any questions or actions from external parties on their analysis work.

The XPRAT will generate analysis plans, status reports, and metrics as required and agreed upon with ESD S&MA and the CPIT.

The XPRAT will establish a process for independent quality assurance of the Cross Program PRA. This assurance will determine compliance of the Cross Program PRA to ESD 10011, Cross Program Probabilistic Risk Assessment Methodology, and NASA NPR 8705.5, Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects, as well as assurance that the model is accurate and complete. NASA policy requires an independent peer review of the PRA to assess methodology and policy compliance; the frequency and proposed level of model maturity required to conduct a peer review will be set forth in the ESD 10011, Cross Program Probabilistic Risk Assessment Methodology document. The XPRAT and all member programs will support the NASA Independent Peer Review (IPR) process, or alternative verification as approved by NASA Office of Safety and Mission Assurance.

8.0 PROGRAM RISK MANAGEMENT

ESD programs are required to comply with NPR 8000.4, Agency Risk Management Procedural Requirements. The ESD Programmatic and Strategy Integration (PSI) team defines the process for integrating program risk management processes and dispositioning integrated risk topics. The process is documented in ESD 10003, ESD Risk Management Plan. The process for managing safety risks is the primary responsibility of Safety and Mission Assurance. Safety and Mission Assurance requirements mandate the development of safety, reliability, and crew survival analyses for the purpose of identifying and assessing safety and mission success Hazards and FMEAs. These items are managed and accepted in accordance with Safety and Mission Assurance Plans. Organizations may, at their discretion, choose to track individual safety risks in the risk management system for the purpose of managing assessment or mitigation activities. For Top Program Risks, the S&MA Technical Authority assures proper identification and inclusion of safety risks in top program risk assessments.

9.0 CERTIFICATIONS

9.1 HUMAN-RATING

ESD programs are required to achieve human rating certification of the integrated space system per NPR 8705.2

S&MA supports the integrated human rating efforts through the development of products required to achieve a human rating certification. These include PRA, IHA, and crew survival analysis. Also, as technical authorities, the CSOs assess the progress of the programs' individual and integrated efforts towards achieving human rating certification and provide recommendations to the programs to facilitate certification. The CSOs provide recommendations to the OSMA Chief regarding human rating compliance at the major milestones. OSMA Chief along with the other TAs and Crew Office (via the JSC Center Director) will provide the official endorsements at these milestones.

9.2 CERTIFICATION OF FLIGHT READINESS (COFR)

ESD will establish an integrated CoFR plan and certification process, which will define S&MA In-Line endorsement responsibilities (ESD 10020, ESD Certification of Flight Readiness (CoFR) Plan). Each Program S&MA organization may define separate CoFR plans to further define processes and responsibilities to fulfill its endorsement responsibilities to its Program Manager, institution, and for integrated CoFR endorsements.

S&MA is required to support the Safety and Mission Success Reviews (SMSR), which is a review held to prepare Agency Safety and Engineering Management to participate in program final readiness reviews preceding flights or launches, including experimental/test launch vehicles, or other reviews as determined by the Chief, Safety and Mission Assurance. The SMSR is co-chaired by the Agency's Chief of S&MA (OSMA) and Chief, Office of Engineering (OCE). The ESD CSO works with OSMA staff to coordinate the SMSR, which provides the knowledge, visibility, and understanding necessary for senior safety and engineering management to either concur or non-concur in program decisions to proceed with a launch or significant flight activity. ESD Programs are required to comply with the requirements for Safety & Mission Assurance (S&MA) Audits, Reviews, and Assessments. The ESD CSO will conduct a pre-brief in order to prepare for the NASA Headquarters-led SMSR as defined in NPR 8705.6, Safety and Mission Assurance (SMA) Audits, Reviews, and Assess. The responsibility for each task/product will be assigned to the appropriate Program or Cross Program Integration (CSI) S&MA organization. Data presented at the NASA Headquarters-led SMSR is developed by the Programs, cognizant NASA Headquarters and NASA Center SMA and engineering organization(s), the NSC, other independent assessment groups (e.g., NESC, NASA IV&V Program, Center-based independent assessment organization), applicable safety review panels, and any individuals or organizations representing minority or dissenting opinions. S&MA will coordinate with the appropriate organizations where S&MA shares task or product responsibilities with other technical authorities (such as Engineering, Health & Medical, or Crew).

APPENDIX A
ACRONYMS, ABBREVIATIONS, AND GLOSSARY OF TERMS

A1.0 ACRONYMS AND ABBREVIATIONS

ADP	Acceptance Data Package
CDR	Critical Design Review
CIL	Critical Item List
CoFR	Certification of Flight Readiness
ConOps	Concepts of Operation
CPIH	Cross Program Integrated Hazard
CPIHA	Cross Program Integrated Hazard Analysis
CPIT	Cross Program Integration Team
CR	Change Request
CSAR	Crew Survival Analysis Report
CSI	Cross Program Systems Integration
CSO	Chief S&MA Officer
CSM	Crew Survival Method
DCR	Design Certification Review
DRM	Design Reference Mission
ECB	ESD Control Board
EM-1	Exploration Mission 1
EM-2	Exploration Mission 2
EOM	End of Mission
ESD	Exploration Systems Development
ESI	Exploration Systems Integration
FAL	Functional Area Lead
FMEA	Failure Modes and Effects Analysis
GMIP	Government Mandatory Inspection Point

GSDO	Ground Systems Development and Operations
GSE	Ground Support Equipment
HERSP	Human Exploration Range Safety Panel
HRCP	Human Rating Certification Package
HQ	NASA Headquarters
ICD	Interface Control Document
IHA	Integrated Hazard Analysis
IHAITT	Integrated Hazard Analysis ITT
IPL	Integrated Product List
ITT	Integrated Task Team
IOZ	Industrial Operations Zones
IPR	Independent Peer Review
IPRA	Integrated Probabilistic Risk Assessment
IRD	Interface Requirements Document
JPCB	Joint Program Control Board
JSC	Johnson Space Center
KSC	Kennedy Space Center
LAS	Launch Abort System
LEO	Low Earth Orbit
LOC	Loss of Crew
LOM	Loss of Mission
LOV	Loss of Vehicle
MPCV	Multi-Purpose Crew Vehicle
MRB	Material Review Board
MPCP	Mishap Preparedness and Contingency Plan
NASA	National Aeronautics and Space Administration
NPRs	NASA Procedural Requirements

ODAR	Orbital Debris Assessment Report
OMRS	Operations and Maintenance Requirements and Specifications
OPR	Office of Primary Responsibility
OSMA	Office of Safety and Mission Assurance
PDR	Preliminary Design Review
PRA	Probabilistic Risk Assessment
PRACA	Problem Reporting and Corrective Action System
PSI	Programmatic and Strategic Integration
QA	Quality Assurance
QuITT	Quality Integrated Task Team
QMS	Quality Management System
S&MA	Safety and Mission Assurance
SLS	Space Launch System
SDR	System Definition Review
SEMP	Systems Engineering Management Plan
SMSR	Safety and Mission Assurance Success Reviews
SOW	Statement of Work
SRR	System Requirements Review
SS	System Safety
SSAR	System Safety Analysis Report
SS ITT	System Safety Integrated Technical Team
SVTL	Safety Vehicle Tracking Log
TA	Technical Authority
TPM	Technical Performance Measurement
XP	Cross Program
XPRAT	Cross Program Probabilistic Risk Assessment Team

A2.0 GLOSSARY OF TERMS

Term	Description
CPIH	A CPIH is defined as any hazard in which more than one program is a contributing cause or control for the hazard. For example, CPIHs require more than one program to contribute to the analysis, the interactions/interfaces, and interdependencies of the hazard.
Dissenting Opinion	A substantive disagreement with a decision or action that an individual judges is not in the best interest of NASA and is of sufficient importance that it warrants a timely review and decision by higher level management.
Loss Of Vehicle (LOV)	<TBD-10010-012>
Non-conformance	Non-conformance is defined as a condition of any article, material, or service in which one or more characteristics do not conform to requirements specified in the contract, drawings, specifications, or other approved product description. Includes failures, discrepancies, defects, and malfunctions. A non-conformance results in one of the following actions: • Fix hardware/software to comply • Process Waiver if against requirements of functional and operational capabilities • Process Deviation if against IRD/ICD, specification, drawing, etc.
Permanent-Disabling Injury -	An injury resulting in permanent impairment/disability of a critical part of the body.
Program Only Hazard	A hazard that is not a CPIH by definition is a Program Only Hazard

APPENDIX B
OPEN WORK

B1.0 TO BE DETERMINED

Table B1-1 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 carets. The TBD item is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<TBD-XXXXX-001>** is the first undetermined item assigned in the document). As each TBD is resolved, 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 B1-1 TO BE DETERMINED ITEMS

TBD	Section	Description
TBD-10010-009	4.1.2.9	MOD OCAD
TBD-10010-011	4.4.1	Secondary Payload Safety Review process being developed by SLS and Orion MPCV.
TBD-10010-012	Appendix A 2.0	Definition of Loss of Vehicle
TBD-10010-015	2.2	ESD 10004 ESD Mishap Preparedness and Contingency Plan (not baselined)
TBD-10010-016	2.2	ESD 10020 ESD Certification of Flight Readiness (CoFR) Plan (not baselined)
TBD-10010-017	Appendix G	Cross Program Material Review Board Charter

B2.0 TO BE RESOLVED

Table B2-1 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 carets. The TBR issue is numbered based on the document number, including the annex, volume, and book number, as applicable (i.e., **<TBR-XXXXX-001>** is the first unresolved issue assigned in 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 B2-1 TO BE RESOLVED ISSUES

TBR	Section	Description

B3.0 FORWARD WORK

The table Forward Work lists the planned Forward Work that the System Safety team will perform. This table is included to acknowledge that this work is ongoing throughout the upcoming Rev B cycle, which is intended to be complete by the ESD Build to Sync (BTS) milestone. As each FW is resolved, the updated text is inserted in the document and the issue is removed from this table. Forward work includes activities that were not completed due to the timely availability of required information, or that required decisions that were pending at the time for Rev A.

TABLE B3-1 FORWARD WORK

Item	Section	Description
Payload Safety	4.4	Rev A and B deals with Secondary Payloads for EM-1 only. Rev C will expand to ESD Payload Safety Process
The cross program MRB process needs to be documented in ESD 10010	6.1.2	The Quality Assurance task team will complete this work in Rev C.
The cross program MRB charter needs to be documented in ESD 10010	Appendix G	Cross Program Material Review Board Charter

APPENDIX C
SAFETY TOPICS

SECTION 1: HAZARD RISK REDUCTION ORDER OF PRECEDENCE

The primary method for minimizing hazards/risks is through a control strategy that will prevent the occurrence of the hazard/risk or reduce the residual risk to an acceptable level by either reducing the likelihood of occurrence or reducing the severity of the hazard.

To eliminate or control hazards, the Programs will use the following hazard reduction precedence sequence:

a. Eliminate hazards by design: Hazards will be eliminated by vehicle design where possible

b. Design for minimum hazards: The major goal throughout the design phase will be to ensure inherent safety through the selection of appropriate design features such as fail-operational/fail-safe combinations and appropriate safety factors. Damage control, containment, and isolation of potential hazards will be included in design considerations.

c. Provide Caution and Warning Devices: Where it is not possible to preclude the existence or occurrence of a known hazard, devices will be employed for the timely detection of the condition and the generation of an adequate warning signal. Warning signals and their application will be designed to minimize the probability of wrong signals or of improper personnel reaction to the signal.

d. Develop and implement Special Procedures: Where it is not possible to reduce the magnitude of existing or potential hazard risks through design, or the use of safety and warning devices, special procedures will be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations will be standardized. The need for hazard detection and safing by the flight crew will be minimized and implemented only when an alternate means of reduction or control of hazardous conditions is not available. With Program approval, real-time monitoring and hazard detection and safing may be utilized to support control of hazardous functions provided that adequate crew response time is available and acceptable safing procedures are developed.

e. Provide personal protective clothing and equipment.

SECTION 2: HAZARD REPORT DATA ELEMENTS

Hazard Data Element	Report Level Description
Hazard Number	Identification of the Hazard Report unique within the program/element/subsystem. This unique identification is assigned to each specific Hazard Report and is never reassigned or reused. The hazard report number will be traceable from the initial identification of the hazard through its resolution and any updates. (EXAMPLE CSHR-05.B.PDR, where CSHR-05 = Core Stage Hazard Report Number 5, B = Revision, and PDR = the traceable delivery).
Hazard Title	Provide a descriptive title of the hazard to give insight into the scope of the Hazard Report. The title should include the hazard and any major defining cause and effect.
Mission Phase(s)	Identify and document the applicable mission phase(s) in which the hazard could manifest. Note that this may not necessarily be the same as the mission phase(s) in which the hazard causes occur. The hazard analysis will use the following mission phases (as applicable): a. Pad Operations and Launch-Hazard analysis begins at start of cryogenic tanking to T-0 umbilical separation b. Ascent-T-0 umbilical separation through placement of Orion in stable Earth orbit c. LEO and TLI Operations-Placement of Orion in stable Earth orbit through trans-lunar propulsion stage disposal d. SLS Post-Ascent Operations –(Recovery/Disposal) Program/Element hazard reports may utilize different mission phase descriptions as long as they are inclusive of and can be mapped to the mission phases specified above and are consistent with ESD 10012, ESD Concept of Operations.
Hazardous Condition Description	The description of the hazardous condition defines the event or condition, fully describes the scenario and hazardous events that must be controlled, and identifies the local effort(s), intermediate effects (e.g., damage to XYZ assembly, subsystem becomes inoperable, etc.) and the worst case effects or results of the hazardous event. Include a description in terms of one or more generic hazards (i.e., fire/explosion, impact, toxicity, etc.). The description should be made explicit to specify the equipment involved. If the hazard is for off-nominal conditions, note the assumptions that were made.

Hazard Data Element	Report Level Description
Acceptance Rationale	Provide a summary of the rationale for accepting the risk associated with the Hazard Report commensurate with the maturity level of hazard analysis performed. Summary should include an overview of the control strategy utilized.
Likelihood Justification	Provide rationale for the likelihood level provided based on control level.
Risk of each cause identified in 5X5 risk matrix	A risk matrix will be completed for each Hazard Report by entering each of the causes (or number of causes if too numerous) into the matrix shown in Figure 4.1-1, thereby documenting each hazard cause severity and likelihood of occurrence. Only causes identified in the Cause Summary will be entered into the matrix.
Hazard Cause Title	The title should briefly describe the root or symptomatic reason for the occurrence of a hazardous condition.
Hazard Cause Description	Provide a description of Hazard causes down to the level at which controls are to be applied. Consider environments, software errors, hardware failures, secondary failures/conditions, procedural errors, operationally induced external and internal failures, FMEA/CIL failure causes, and human errors/limitations when developing the description. Include a description of the cause effects.
Likelihood of Occurrence	Hazard likelihood is the probability that an identified hazard cause will occur and result in the hazardous effect in a single mission. The controls are considered to be in place when performing the likelihood of occurrence assessment. Classify the likelihood for each cause by assessing the controls that are in place and documenting the likelihood as very high, high, low or very low as defined in Table 4.1-2.
Likelihood Justification	Provide a summary of the rationale for classification of the likelihood. Include assumptions, any empirical data, a qualitative summary of the failure history, and any uncertainties, confidence factors, or limitations (including applicable waivers) 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 likelihood relative to the other causes within the Hazard Report, additional rationale will be necessary to support that classification. PRACA data should be consulted for qualitative failure history when determining the likelihood. The time parameter for assessing the likelihood is for the mission under analysis. Update the rationale and classification at each design milestone review based upon the evaluation of the successful implementation of the control and verification strategy.

Hazard Data Element	Report Level Description
Severity	The severity level is an assessment of the worst-case effects of the hazard, assuming no controls are in place. Complete for each cause by assessing the most severe effect and documenting it as catastrophic, critical, severe, moderate, or minor (defined in Table 4.1-3). FMEA/CIL criticality should be consulted when determining the severity.
Control(s)	Document or reference all controls that prevent the occurrence of a hazard cause or reduces the residual risk to an acceptable level. A valid control used to meet failure tolerance requirements must exist such that no single event or common cause failure can result in a potentially hazardous event. Design controls include those attributes of the robustness of the design. Operational controls are generally the least desirable form of hazard control and should be used when design controls are unavailable. Operational controls are implemented via procedures, flight rules, launch commit criteria, or training. . Include a description of all the necessary design/operational controls for this hazard cause, including existing technical requirements (e.g., factors of safety, design standards, etc.), including documentation references, if applicable. To the extent practical, the Hazard Report should include pointers with unique identification(s) to specific test and inspection controls documented in the retention rationale for the applicable CILs in order to minimize duplication. The hazard controls will be numbered (indexed) to provide direct linkages with the appropriate cause and verification(s) within the hazard report as well as with any other hazard report causes that utilize the control(s). For element hazards controlled by other programs and/or elements; provide a direct linkage of each Hazard Report cause with all control(s) relevant to controlling that cause documented in the integrated hazard report.

Hazard Data Element	Report Level Description
Verifications	Provide a summary with sufficient detail/explanation of the verification methods (testing, inspection, analysis, etc.), which assure the identified controls are present, adequate, and effective, and support hazard closure or risk acceptance rationale. CIL retention rationale verifications will be identified where appropriate to assure consistency between the hazards and the FMEA/CILs. FMEA/CILs may be referenced by unique identification number to avoid duplicating information. Verifications will be performed by the contractor, government, or both. Identify and document specific verification types including analyses, tests, inspections, and/or demonstration for each verification activity. Each verification type will be indexed with its corresponding hazard cause (PDR), and control (CDR, DCR). When more than one type of verification is listed for a control, the verification types and status will be listed with a unique identifier. Traceability to the specific control information is required. The required documentation of verification activities progresses with the maturity of the design as follows: • PDR – Identify and document the specific verification type (i.e., test, analysis, inspection, or demonstration) applicable to each hazard cause as well as a description of the planned verification activities which outline the overall verification strategy providing enough detail to facilitate classification of the likelihood of the hazard. • CDR – Completion of document number or completion plan with ECD of verification activities to assure the effectiveness of each hazard control is identified and required for the CDR Delivery. • DCR – Design Certification Review, document completed hazard control verifications, including reference to specific documents (test reports, analysis reports, etc.) where control verification is demonstrated. A verification tracking log or other traceability tool will reference each verification to an approved Element/Program document to ensure effective implementation of the controls.
Crew Survival Methods	Program integrated hazard analyses must identify Crew Survival Methods (CSMs) that will increase the probability of crew survival in the event that all hazard controls have failed and the catastrophic event is imminent. Within the program integrated hazard analysis, the planned CSMs (e.g. Abort, Escape, Emergency Egress, Safe Haven, Rescue, Emergency Medical, Other, or None) should be identified, a description provided if not evident by the survival method identified, and reference provided to documentation or analysis that verifies the adequacy of the survival method identified.

APPENDIX D
MILESTONE REVIEW SUCCESS CRITERIA FOR ESD INTEGRATED HAZARD ANALYSIS

The following criteria constitute the minimum content for ESD integrated hazard analysis packages required as input to the hazard analysis review process described in Section 4.1 for a given milestone. Note that these criteria apply to the final ESD system safety package review for a given milestone.

Success Criteria for System Requirements (SRR)/System Definition Review (SDR) Milestone:

Content for the SRR and SDR timeframe is as follows:

a. Scope and Objective
b. Organizational Structure
c. Interface Overview
d. Overview, Ground Rules, & Assumptions
e. Hazard Analysis Approach
f. Approach for Controlling Hazards (Failure Tolerance, exception (e.g. structures))
g. Special Topics (including any Areas of Concern)
h. Forward Plan for Preliminary Design Review (PDR) Milestone
i. Initial set of hazard analysis topics
j. Initial set of risk areas based on discussions with Engineering

Success Criteria for Preliminary Design Review (PDR)

The PDR will be considered complete and successful when the milestone review board and TAs concur that the following hazard products are at a PDR maturity level:

a. Developed list of hazardous conditions with supporting graphical representation of relationship between hazardous conditions and causes consistent with the level of PDR design definition
b. Description and effect(s) for each hazardous topic has been developed and is consistent with the level of PDR design definition
c. Hazard cause(s) have been identified consistent with the level of PDR design definition
d. Elimination/Mitigation strategies or preliminary controls for the hazard causes consistent with the level of PDR design definition
e. Failure Tolerance/Exception Approach has been identified for applicable hazard causes and is consistent with the level of PDR design definition

f. Preliminary verification methods for each hazard control have been identified consistent with the level of PDR design definition

g. Potential Crew Survival Methods (CSM) for catastrophic hazards has been identified and descriptions of their role in ensuring crew survival are provided

h. All action items/RIDs required to be closed for PDR have been dispositioned

i. Updated list of risk areas

Success Criteria for Critical Design Review (CDR)

CDR will be considered complete and successful when the milestone review board and TAs concur that the following hazard products are at a CDR maturity level:

a. Updated list of hazardous conditions areas with graphical representation of relationship between hazardous conditions and causes consistent with the level of CDR design definition

b. All hazard causes have identified through the Hazard analysis. (Hazard causes have been updated as a result of design changes and/or analysis maturity since PDR)

c. All controls for the hazard causes are acceptable as documented and as implemented in the hardware/software design

d. Verifications for the hazard controls are acceptable as documented in the hazard products

e. CSMs for catastrophic hazards have been identified, descriptions of their role in ensuring crew survival are provided, and reference to the documentation/analysis that verifies the availability of the identified CSMs is included

f. All action items/RIDs required to be closed for CDR have been dispositioned

g. Updated list of risk areas

h. Assessment to ensure a complete set of all hazardous conditions and causes

i. Preliminary risk ranking

Success Criteria for Design Certification Review (DCR)

DCR will be considered complete and successful when the following hazard products are approved/baselined:

a. All hazard causes have been identified through the fault tree analysis (or other appropriate analysis). Hazard causes should be updated as a result of the design changes and/or analysis maturity since CDR

b. All controls for the hazard causes are acceptable as documented in the hazard products and as implemented in the hardware design

c. All hazard control verifications have been completed or a closure plan and ECD accepted

d. All data used for acceptance rationale and justifications for the risk classifications have been sufficiently identified and documented

e. CSMs for catastrophic hazards have been identified, descriptions of their role in ensuring crew survival are provided, and reference to the documentation/analysis that verifies the availability of the identified CSMs is included

f. All action items/RIDs required to be closed for DCR have been dispositioned

g. All required hazard products are complete and accurate

h. Updated assessment to ensure a complete set of all hazardous conditions and causes

i. Updated list of risk areas (residual risks)

APPENDIX E
CONTENT AND MATURITY CRITERIA FOR THE CROSS PROGRAM CREW SURVIVAL ANALYSIS REPORT

NPR 8705.2B, Human Rating Requirements for Space Systems, requires certain information regarding crew survival to be included in the Human Rating Certification Package (HRCP). The appendix specifies the content of the Cross Program Crew Survival Analysis Report (CSAR) at various milestones. References to the NPR indicate required content for the HRCP.

TABLE E-1 CSAR CONTENT AND MATURITY CRITERIA FOR SRR/SDR

Content	NPR 8705.2B Reference
a. Scope and Objective	
b. Analytical Approach./Methodology & Assumptions	
c. Design reference mission overview	
d. Summary of planned crew survival strategies/methods	2.3.2
e. Summary of known LOC hazards	
f. Crew Survival Coverage Analysis • CS capabilities by phase • CS capabilities by major system hazard • Hazard-CS strategy trace by mission phase • CS gaps	 2.3.4 2.3.2
g. Trace of CS strategies to requirements and capabilities	2.3.4
h. Recommendations and Open Questions	
i. Forward Work	

TABLE E-2 CSAR CONTENT AND MATURITY CRITERIA FOR PDR

Content	NPR 8705.2B Reference
a. Scope and Objective	
b. Analytical Approach/Methodology & Assumptions (applicable to this phase)	
c. Design reference mission overview	
d. Summary of planned crew survival strategies/methods (update noting changes since SDR)	2.3.2
e. Summary of known LOC hazards	
f. Crew Survival Coverage Analysis (update) • CS capabilities by phase • CS capabilities by major system hazard • Hazard-CS strategy by mission phase • CS gaps	 2.3.4 2.3.2
g. Summary of other changes since SRR/SDR	
h. Trace of CS strategies to requirements and capabilities (update)	2.3.4
i. Crew survival effectiveness matrix, including probabilistic risk assessment results	2.3.7.1 d
j. Recommendations and Open Questions	
k. Forward Work	

TABLE E-3 CSAR CONTENT AND MATURITY CRITERIA FOR CDR

Content	NPR 8705.2B Reference
a. Scope and Objective	
b. Analytical Approach/Methodology & Assumptions (applicable to this phase)	
c. Design reference mission overview	
d. Summary of planned crew survival strategies/methods (update noting changes since PDR)	23.2
e. Summary of known LOC hazards	
f. Crew Survival Coverage Analysis (update) • CS capabilities by phase • CS capabilities by major system hazard • Hazard-CS strategy by mission phase • CS gaps	 2.3.4 2.3.2
g. Summary of crew survival capabilities V&V approach • Level of verification (e.g., complete certification, no verification) • Verification methods (test, analysis, etc.)	2.4.2
h. Summary of other changes since PDR	
i. Trace of CS strategies to requirements and capabilities (update)	2.3.4
j. Crew survival effectiveness matrix, including probabilistic risk assessment results	2.3.7.1 d
k. Recommendations and Open Questions	
l. Forward Work	

TABLE E-4 CSAR CONTENT AND MATURITY CRITERIA FOR DCR/ORR

Content	NPR 8705.2B Reference
a. Scope and Objective	
b. Analytical Approach/Methodology & Assumptions (applicable to this phase)	
c. Design reference mission overview	
d. Summary of planned crew survival strategies/methods (update noting changes since CDR)	23.2
e. Summary of known LOC hazards	
f. Crew Survival Coverage Analysis (update) • CS capabilities by phase • CS capabilities by major system hazard • Hazard-CS strategy by mission phase • CS gaps	 2.3.4 2.3.2
g. Summary of crew survival capabilities V&V results • Level of verification (e.g., complete certification, no verification) • Verification methods (test, analysis, etc.)	2.4.2
h. Summary of other changes since CDR	
i. Trace of CS strategies to verification data	2.3.4
j. Crew survival effectiveness matrix, including probabilistic risk assessment results	2.3.7.1 d
k. Recommendations and Open Questions	
l. Forward Work	

APPENDIX F
CLARIFICATION OF FAILURE TOLERANCE APPLICABILITY TO HAZARD CAUSES

The failure tolerance requirement imposed on ESD and its constituent programs is derived directly from NPR 8705.2B, Human Rating Requirement for Space Systems, paragraph 3.2.3. This requirement levies minimum failure tolerance levels for the “space system” as defined in Appendix A of the NPR as the collection of all space- and ground-based systems encompassing hardware and software used to conduct or support activities in space.

In some cases, the hazard analysis targets potentially hazardous conditions that result from factors other than the performance of the hardware or software that makes up the “space system”. For example, hazard causes may be written against inadequate or improper engineering analysis performed to predict the system’s behavior or to derive system design or operational requirements. Such hazard causes are focused on the engineering processes for performing, controlling, approving, and documenting the engineering analysis and results rather than on the hardware/software of the space system.

Other areas covered by hazard analysis may fall into similar categories where the engineering and management processes are the target of assessment rather than the actual space system.

With consideration to both the wording and intent (as stated in the rationale) of the human rating failure tolerance requirement in 3.2.3.b of NPR 8705.2B, referred to as the “ Part b exception” this exception to the failure tolerance requirement is determined to apply to all ESD hazards or hazard causes that can be categorized as shown in Table F-1. The hazard causes listed are general – actual hazard or hazard cause titles may differ from the causes listed below although they are similar in scope and the approach to controlling them.

Technical Authority representatives participating in review of ESD cross program or program hazard analysis will assure the applicability of this clarification to any hazards under review. Hazards will be accepted through the hazard review process.

TABLE F-1 HAZARD CAUSES THAT ARE EXCEPTED FROM FAILURE TOLERANCE BASED ON NPR 8705.2B

Hazard Cause: • Improper or inadequate analysis or models; Improper or inadequate design definition; Improper or inadequate operational requirements or procedures
Description: • Inadequate, erroneous, or missing analysis can result in flawed design or operational requirements. • Improper/inadequate validation of models can yield inaccurate analytical results. • Inadequate control of analytical and modeling processes (configuration management, peer review, approval or results, etc.) can yield flawed results. • Improper flow-down of analytical results into system design or operational requirements/procedures can result in flawed design or operation of the system outside its analyzed capabilities.
Control Approach: • Identify critical analyses and models used in integrated design analyses. • Assure level of controls placed on analyses and models are commensurate with risk of erroneous results. • Assure validation approach including heritage, testing, and independent/peer review are adequate. • Identify critical inputs required from other programs to program performing/leading analysis. • Assure appropriate natural and induced environments are accounted for in the analysis. • Assure critical results, constraints, or assumptions are accounted for in design and operational requirements.

Hazard Cause: • Improper or inadequate definition of environments
Description: • Inadequate or incorrect derivation, documentation, and flow-down of induced and natural environments needed to design the system results in inadequate certification/qualification of the space system. • Inadequate or erroneous prediction of weather environments can result in operation of system outside certified limits during launch or flight.
Control Approach: • Assure accurate characterization of environments based on historical data or comprehensive analysis. • Assure environments are documented and flowed to programs as design-to criteria. • Assure appropriate operational constraints or criteria are in place.

Hazard cause: • Improper system configuration
Description: • Errors in assembly, integration, or test of the space system due to improper operational requirements or instructions can result in uncertified system configuration.
Control Approach: • Assure operational requirements, drawings, instructions, etc., are in place and configuration managed.

APPENDIX G
CROSS PROGRAM MATERIAL REVIEW BOARD CHARTER

The Cross Program Material Review Board Charter will be documented in this appendix. The charter will be drafted by the Quality Assurance ITT as forward work for the Revision C CR.