

National Aeronautics and
Space Administration

SLS-RQMT-015

BASELINE

RELEASE DATE: OCTOBER 28, 2011

SPACE LAUNCH SYSTEM (SLS) PROGRAM HAZARD ANALYSIS REQUIREMENTS

Approved for Public Release; Distribution is Unlimited.

*The electronic version is the official approved document.
Verify this is the correct version before use.*

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 2 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

REVISION AND HISTORY PAGE

| Status | Revision No. | Change No. | Description | Release Date |
|----------|--------------|------------|--|--------------|
| Baseline | – | | Baselined by Space Launch System Program Control Board Directive SV2-01-0002 (PCN SV00002, CR SLS-00002) | 10/28/11 |

NOTE: Updates to this document, as released by numbered changes (Change XXX), are identified by a black bar on the right margin.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 3 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

TABLE OF CONTENTS

| PARAGRAPH | PAGE |
|---|-------------|
| 1.0 INTRODUCTION | 5 |
| 1.1 Purpose..... | 5 |
| 1.2 Scope..... | 5 |
| 1.3 Change Authority/Responsibility..... | 5 |
| 1.4 Hazard Analysis Interrelationship with the FMEA/CIL..... | 6 |
| 2.0 DOCUMENTS..... | 7 |
| 2.1 Applicable Documents..... | 7 |
| 2.2 Reference Documents | 7 |
| 3.0 HAZARD ANALYSES REQUIREMENTS | 8 |
| 3.1 Hazard Analyses | 10 |
| 3.1.1 Element Hazard Analyses (EHAs) | 10 |
| 3.1.2 SLS Program Integrated Hazard Analyses (IHAs)..... | 12 |
| 3.1.3 Cross-Program Integrated Hazard Analyses | 13 |
| 3.1.4 System Safety Analysis Report | 18 |
| 4.0 HAZARD ANALYSIS DATA DELIVERY REQUIREMENTS | 20 |
| 4.1 Hazard Analysis Review Process Requirements | 21 |
| 4.1.1 SLS Hazard Analysis Review Process Overview | 21 |
| 4.1.2 Element Hazard Analysis Review | 21 |
| 4.1.3 Program Integrated Hazard Analysis Review | 22 |
| 4.1.4 Other In-House Safety Analysis Review (e.g., Payload Adaptor) | 22 |
| 4.1.5 In-Between Milestone Reviews..... | 22 |
| 4.2 Hazard Risk Acceptance and Approval Requirements..... | 23 |
| 4.2.1 Controlled Risk (Green) | 24 |
| 4.2.2 Accepted Risk (Yellow) | 25 |
| 4.2.3 Red Risk | 25 |
| 4.2.4 Top Right Box..... | 25 |
| 4.3 Maintaining Hazard Reports Current..... | 26 |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 4 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

4.4 Definitions.....26

APPENDIX

APPENDIX A ACRONYMS AND ABBREVIATIONS28

APPENDIX B OPEN WORK30

TABLE

TABLE 3-1. HAZARD REPORT DATA ELEMENTS14

TABLE 4-1. HAZARD ANALYSIS DELIVERY SCHEDULE20

TABLE 4-2. HAZARD LIKELIHOOD DEFINITIONS24

TABLE 4-3. HAZARD SEVERITY DEFINITIONS24

TABLE B1-1. TO BE DETERMINED ITEMS30

FIGURE

FIGURE 4-1. DELEGATED HAZARD RISK ACCEPTANCE MATRIX23

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 5 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to set forth the requirements and processes required for the Space Launch System (SLS) Program and Elements in implementing a robust hazard analysis, development, review, and approval process.

This document provides requirements for conducting the hazard analyses for the SLS Program and Elements including any government furnished equipment (GFE) and ground support equipment (GSE) developed for these entities. The safety requirements established for the SLS Program dictate that comprehensive and accurate safety analytical practices be developed and implemented to identify and document all hazards and their associated causes, controls and verifications, and an assessment of the residual safety risk.

The Program and Element data requirement delivery documents will reference this document for Hazard Analysis Requirements.

1.2 Scope

The SLS Program and Elements are responsible for identifying all hazards and hazard causes associated with flight and ground hardware (including GSE and GFE) that manifest during preflight processing on the launch pad and during flight of the Space Launch System from design, development, manufacturing/construction, testing, transporting, maintenance, ground processing, and operations activities. The hazard analysis is initiated during the formation and design concept phase and continuously matured throughout the Program life cycle as designs evolve and operations commence (e.g., manufacturing, processing, testing, flights).

This document contains programmatic requirements for the content, definition, delivery, and approval of hazard analyses for the SLS Program. Other SLS Safety and Mission Assurance (S&MA) Program requirements can be found in SLS-RQMT-014, SLS Program S&MA Requirements Document. Cross-program S&MA programmatic requirements can be found in the ESD-PLAN-**<TBD-001>**, Cross-Program S&MA Plan. The SLS technical (“design to” type) S&MA requirements are contained in SLS-SPEC-032, Space Launch System Vehicle Specification, and subordinate documents.

1.3 Change Authority/Responsibility

The appropriate NASA Office of Primary Responsibility (OPR) identified for this document is the Marshall Space Flight Center (MSFC) Safety and Mission Assurance (S&MA) Directorate.

Proposed changes to this document shall be submitted by an SLS Program Change Request (CR) to the SLS Program Control Board for consideration and disposition. All requests will be processed in accordance with SLS-PLAN-008, Space Launch System Program Configuration

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 6 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

Management (CM) Plan. Any changes shall require approval, at the SLS Program Control Board, by the SLS Chief S&MA Officer (CSO) as the S&MA Technical Authority (TA).

1.4 Hazard Analysis Interrelationship with the FMEA/CIL

The Safety Hazard Analysis and Failure Modes and Effects/Critical Items List (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 SLS design. 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 control and verification of hazard causes. At the discretion of the hardware developer, controls and verifications for hardware failure modes may be documented either directly in the applicable hazard reports or through reference to specific FMEA/CIL retention rationale.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 7 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

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. Unless otherwise stipulated, the most recently approved version of a listed document shall be used. In those situations where the most recently approved version is not to be used, the pertinent version is specified in this list.

| | |
|--------------------|--|
| SLS-RQMT-014 | Space Launch System (SLS) Program Safety and Mission Assurance (S&MA) Requirements |
| SLS-SPEC-032 | Space Launch System Vehicle Specification |
| ESD-PLAN-<TBD-004> | Cross-Program S&MA Plan |
| SLS-PLAN-008 | Space Launch System Program Configuration Management Plan |

2.2 Reference Documents

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

| | |
|---------------------------------|---|
| SAE ARP4761 | Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment |
| MIL-STD-882 | System Safety Program Requirements |
| NASA Reference Publication 1358 | System Engineering “Toolbox” for Design-Oriented Engineers |
| NSTS 22254 | Methodology for Conduct of Space Shuttle Program Hazard Analyses |
| CxP 70038 | Constellation Program (CxP) Hazard Analyses Methodology |
| | Federal Aviation Administration (FAA) System Safety Handbook |
| SLS-RQMT-016 | Space Launch System (SLS) Program Failure Modes and Effects Analysis/Critical Items List Requirements |
| SLS-SPEC-<TBD-005> | Abort Conditions Report |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 8 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

3.0 HAZARD ANALYSES REQUIREMENTS

Exploration Systems Directorate (ESD) programs are required to comply with NPR 8705.2B, Human-Rating for Space Systems. NPR 8705.2B establishes requirements for minimum failure tolerance for prevention of catastrophic hazards. The SLS Program shall establish hazard control requirements and verification of the controls for catastrophic and critical hazards using NPR 8705.2B as a minimum requirement. The SLS Program/Element Offices shall establish System Safety activities including hazard analyses (HAs) to answer those requirements. This document contains programmatic requirements that answer requirements in NPR 8705.2B. The technical requirements in NPR 8705.2B are met by SLS-SPEC-032, Space Launch System Vehicle Specification, and subordinate documents.

The analysis shall address all hazards and hazard causes associated with flight and ground hardware (including GSE and GFE) that manifest during preflight processing on the launch pad and during flight from design, development, manufacturing/construction, testing, transporting, maintenance, ground processing, and operations activities. Hazard analysis shall be performed at the SLS Program and Element levels.

Note that these requirements for the delivery and review of hazard analyses should be applied to the certification of flight configuration hardware of an element. Also, the design milestone reviews referenced in these requirements are pertaining to the element and integrated program level milestone reviews (System Definition Review (SDR), Preliminary Design Review (PDR), Critical Design Review (CDR), & Design Certification Review (DCR)) as shown in Table 4-1, and not to its individual subsystems/components.

The analysis shall identify integrated hazards created and/or controlled by the SLS Program and/or Elements that impact other Programs and/or others (International Space Station (ISS), public, international partners, etc.). (Reference Section 3.1.3 Cross-Program Integrated Hazard Analyses.)

The SLS Program and Elements shall initiate hazard analysis during the conceptual phases and continue to mature the analyses throughout the life cycle of the Program.

The SLS Program and Elements shall establish a formal, closed-loop, risk acceptance process to identify and track hazards with residual risk and communicate those risks to the Program for acceptance at each milestone review to ensure that all hazards and risks identified in the HAs are either eliminated or controlled to acceptable levels.

All hazard reports (HRs) and system safety analysis reports (SSARs) shall be electronically deposited in accordance with the delivery requirements in Section 4.0 into the Program's Hazard Database beginning at the Program and Element PDRs. The following electronic formats are acceptable (Microsoft Word, Excel, PowerPoint, and PDF).

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 9 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

Beginning at PDR, the SLS Program and Elements shall ensure at each integrated vehicle and element design milestone review that all hazardous conditions or other safety issues have been identified and a control and verification strategy is identified appropriate to the hazard level.

The SLS Program and Elements shall demonstrate verification of successful hazard control implementation by SLS systems, elements, subsystems, components, and subcomponents by inspection, test, demonstration, and/or analysis. Verification activities shall demonstrate that risk mitigation and hazard controls have been implemented and are effective. Hazard reports will reference existing vehicle verification documentation to track hazard closure. The requirements (shall statements) within this document do not require a formal verification plan but are subject to documentation review/approval, audit, surveillance, and inspection activities.

The SLS Program and Elements will include interaction early in the design and development cycle (System Requirements Review (SRR), PDR) between system safety, engineering, integration, and operations functions to ensure all hazards are identified and documented.

In order to ensure that the residual safety risk inherent in the design is well understood and controlled, the HAs shall be baselined and placed under formal configuration management control no later than 30 days prior to the Element and Program DCR.

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 SLS Program and Elements shall use the following hazard reduction precedence sequence:

- a. **Eliminate Hazards By Design** – Hazards identified in the relevant hazard analyses will be eliminated by 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. **Incorporate Safety Devices** – Known hazard risks, which cannot be eliminated through design selection, will be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment.
- d. **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

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 10 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

signals and their application will be designed to minimize the probability of wrong signals or of improper personnel reaction to the signal.

- e. **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. While the preferred method for hazard detection and safing is through design and use of automatic controls, additional flight crew in the loop controls may be added when automation is not possible and override of automatic operations is deemed necessary by the flight crew. 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.
- f. **Provide personal protective clothing and equipment.**

Hazard Analysis Reference Tools

Additional reference sources for performing hazard analyses are included in the Reference Document list (reference Section 2.2) such as CxP 70038, Constellation Program Hazard Analyses Methodology. These references are examples of sources for locating tools and methods for the performance of the hazard assessment.

Fault Tree Analyses (FTAs) or equivalent logic analyses have historically been preferred for evaluating the effects of individual and multiple hardware and software faults, interfaces, environmental conditions, and human error on launch vehicle systems. Methods for performing these analyses can be found in the Reference Document list (reference Section 2.2).

3.1 Hazard Analyses

The Elements shall perform and document hazard analyses as described below:

3.1.1 Element Hazard Analyses (EHAs)

The Elements shall perform an element hazard analysis which includes an SSAR (as defined in Section 3.1.4) and a set of hazard reports. Hazard reports are documented as one report for each hazard or multiple close-coupled hazards with a similar control strategy. Element hazard reports document all hazards and hazard causes to the element and all hazards and hazard causes which the element may cause to another element or program. Each report shall address the hazard causes and the corresponding control and verification strategy appropriate to the severity level of that hazard. Elements are also responsible for the EHA applicable to the integration of GFE and GSE. Each report shall contain the data elements as defined in Table 3-1. Elements shall classify the risk of the hazard occurrence for each hazard and hazard cause, excluding those causes

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 11 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

controlled by other Programs and/or Elements, according to the hazard risk matrix in Figure 4-1 and the likelihood and severity definitions in Tables 4-2 and 4-3, respectively. Element hazard reports shall document when other elements rely on controls within their hazard report(s) in each applicable cause control summary. Element hazard causes that are controlled by other programs or elements shall be identified as a program integrated hazard and referenced to the corresponding program integrated hazard report. Risk for Element hazard causes controlled by other programs is classified in the program integrated hazard report (Section 3.1.2). Note: For hazard scenarios that result only from a combination of hazard causes, the assignment of likelihood and severity can be made at a higher level than the individual causes. Risk is accepted by the Elements, the Program, the ESD Manager, or by the NASA Administrator as shown in Figure 4-1. The EHA should consider the following analyses as source data for the hazard reports.

- **Element Subsystem Hazard Analysis** – The analysis of element component functions and their contribution to an element hazardous effect.
- **Operating and Support Hazard Analysis (O&SHA)** – The O&SHA provides a detailed safety risk assessment of a system’s operational and support procedures during all phases of intended system/hardware/facility use.
- **Software Hazard Analysis** – Software plays an important role in the control and monitoring of system hazards. Software hazard analyses will take place during all phases of system development and will be incorporated at the appropriate system hazard analysis level throughout the life of the program. Software has system-wide implications often providing the control and monitoring across elements and systems, and as such, needs to be analyzed from the software system perspective, as well as the integrated system. While subsystem software hazard analyses are performed, the impact within and across elements needs to be analyzed as well. Thus, software hazard analyses will need to flow both up and down through the system and may be performed at several levels.
- **Human Error Analysis** – The human error analysis ensures that human factors engineering principles are applied to the design to eliminate or control potential hazard risks associated with the human–system interfaces. The human error analysis is used as source data for the formal hazard analysis. The Program and Element hazards associated with human error are controlled according to the following stated order of precedence. Justification rationale for the exclusive utilization of controls described in item c is included in the associated hazard report:
 - a) The system design prevents human error.
 - b) The system reduces the likelihood of human error and provides the capability for the human to detect and correct the error through the incorporation of systems, controls, and associated monitoring.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 12 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

- c) The system provides a method to limit the negative effects of errors so that the error does not result in a fatality or permanent disability.

3.1.2 SLS Program Integrated Hazard Analyses (IHAs)

The Program shall perform and document hazard analyses as described below:

Integrated Hazard Analysis (IHA) is a top-down assessment of all Program and Element hardware, ground support hardware, software, and operational interactions that identify both the undesired events (hazards) that can result from those interactions as well as how those events are controlled, including those cases for which multiple Programs and/or Elements provide controls (i.e., hazards caused by one Program or Element that affect another Element or Program). The Element hazard reports reference the appropriate integrated hazard report when there is a related integrated hazard in another element.

The Program shall perform an integrated hazard analysis which includes a SSAR (as defined in Section 3.1.4) and a set of hazard reports. Hazard reports are documented as one report for each hazard, or multiple close-coupled hazards with a similar control strategy. Program hazard reports document all hazards and hazard causes which involve systems or subsystems that cross programs and/or elements. The IHA will document the control and verification methods for causes that are beyond the responsibility of a single Element.

Each report shall document the hazard, hazard causes, and the corresponding control and verification strategy, appropriate to the severity level of that hazard. Each report shall contain the data elements as defined in Table 3-1. The Program shall classify the risk of the integrated hazard occurrence for each hazard and hazard cause according to the hazard risk matrix in Figure 4-1 and the likelihood and severity definitions in Tables 4-2 and 4-3, respectively. The integrated hazard risk is accepted by the Program, the ESD Manager, or by the NASA Administrator as shown in Figure 4-1. The Program IHA should consider the following analyses as source data for the program integrated hazard reports.

- **Operating and Support Hazard Analysis** – The O&SHA provides a detailed safety risk assessment of a system’s operational and support procedures during all phases of intended system/hardware/facility use.
- **Software Hazard Analysis** – Software hazard analysis takes place during all phases of hazard analyses and is incorporated at the appropriate hazard analysis level. As software’s role in the control and monitoring of the system evolves, software hazard analyses will take place during all phases of system development and be incorporated at the appropriate system hazard analysis level throughout the life of the program. Software has system-wide implications often providing the control and monitoring across elements and systems, and as such, needs to be analyzed from the software system perspective as well as the integrated system. While subsystem software hazard analyses are performed,

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 13 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

the impact within and across elements needs to be analyzed as well. Thus, software hazard analyses will need to flow both up and down through the system and may be performed at several levels.

- **Human Error Analysis** – The human error analysis ensures that human factors engineering principles are applied to the design to eliminate or control potential hazard risks associated with the human–system interfaces. The human error analysis is used as source data for the formal hazard analysis. The Program and Element hazards associated with human error are controlled according to the following stated order of precedence. Justification rationale for the exclusive utilization of controls described in item c is included in the associated hazard report:
 - a) The system design prevents human error.
 - b) The system reduces the likelihood of human error and provides the capability for the human to detect and correct the error through the incorporation of systems, controls, and associated monitoring.
 - c) The system provides a method to limit the negative effects of errors so that the error does not result in a fatality or permanent disability.

The Program shall determine accountability at the cause level for all integrated hazard causes.

- 1) For element causes, the responsible Element is coordinated with to determine the appropriate controls and verification methods and associated HR/CIL documentation that will be referenced in the program integrated hazard analysis.
- 2) For integrated causes, the affected Projects/Elements are coordinated with to determine both the integrated system controls and verification methods and element controls and verification methods. The appropriate project/element HR/CIL documentation will also be determined for referencing in the Integrated Hazard Report.

3.1.3 Cross-Program Integrated Hazard Analyses

Cross-program hazard analysis, data delivery, and documentation shall be conducted in accordance with the process described in ESD-PLAN-**<TBD-007>**, Cross Program S&MA Plan.

Cross-program integrated hazards are defined as any hazard in which more than one program is a contributing cause or control for the hazard, or where unique hazards are created during the assembly or operation of SLS and Multi-Purpose Crew Vehicle (MPCV) or payload together and with other programs.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 14 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

Table 3-1. Hazard Report Data Elements

| The following data elements are documented at the report level for each hazard. | |
|---|--|
| Hazard Report 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 shall be traceable from the initial identification of the hazard through its resolution and any updates. <i>(Example: CSHR-05.B.PDR where CSHR-05 = Core Stage Hazard Report number 5, B = revision, and PDR = the traceable delivery.)</i> |
| Hazard Title | Provide a descriptive title of the hazard to give insight into the scope of the hazard report. The title should include the following information (in this suggested format): "The (system) (does what? What requires control?) resulting in (consequence(s))." |
| Mission Phase | <p>Document the applicable mission phase(s) in which the hazard manifests. Note that this may not necessarily be the same as the mission phase(s) in which the hazard causes occur. The hazard report shall consider the following mission timeline events when identifying the applicable mission phase:</p> <ul style="list-style-type: none"> • Start of cryogenic tanking • Core stage engine start • Booster ignition • Liftoff • Tower clear • Booster separation • Core stage burnout • Core stage to MPCV/payload/second stage separation • Core stage reentry • Second stage engine ignition • Second stage burnout • Second stage to MPCV/payload separation • Second stage reentry <p>The program and elements may choose to utilize logical groupings of the above mission phase events to map to a higher level element- or program-specific mission phase. Mission phases identified in the HA shall be consistent within each element and within all program-level hazard reports.</p> |
| Mission Effectivity | Identify the applicable design reference mission, ground facility, launch pad, or test flight, etc., as appropriate to the scope of the hazard report. |
| 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 effect(s), intermediate effects (e.g., damage to XYZ assembly, subsystem becomes inoperable) and the worst-case effects or results of the hazardous event. Include a description in terms of each applicable hazard type (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. |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 15 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

| | |
|---|--|
| Report Status | <p>Report status is classified as <i>open</i> or <i>closed</i>.</p> <p>Open: Further action(s) to eliminate or control the hazard is required (e.g., analysis, test, or verification of the control).</p> <p>Closed: Action(s) to eliminate or control the hazard have been implemented or incorporated (e.g., design change incorporated, procedure and plans released) and verification of implementation or incorporation has been accomplished.</p> |
| Acceptance Rationale | Provide a summary of the rationale for accepting the risk associated with the hazard report commiserate with the maturity level of hazard analysis performed. Summary should include an overview of the control strategy utilized. |
| Failure Tolerance (FT) to the Hazard | <p>Describe the built-in capability of the system to perform as intended in the presence of specified failure modes. Evaluate each hazard cause and report the case(s) which provide the weakest level of failure tolerance to the hazard, identifying only the failure tolerance level for items that are not exempt according to SLS-SPEC-032, Space Launch Vehicle Specification. The FMEA/CIL will be consulted when assessing failure tolerance.</p> <p>Extravehicular activity (EVA), emergency systems, or emergency operations shall not be considered as contributions to failure tolerance.</p> <p>Those reports that document case(s) that are not meeting the FT requirement must be elevated to the program for a determination of implementing additional controls, to initiate a design change, declare an exception with Technical Authority concurrence, or to process a waiver. Waivers to the FT requirements are to be processed at the program level in accordance with SLS-PLAN-008, SLS CM Plan. The Program Manager, Program CSO, and Program Chief Engineer (CE) will have the minimum level of approval for those reports.</p> |
| Hazard Cause Summary | Provide a listing of all the causes developed within the hazard report and indicate the severity and likelihood for each cause; also list any previously considered hazard causes eliminated by design. |
| Hazard 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, thereby documenting each hazard cause severity and likelihood of occurrence. Only causes identified in the Cause Summary will be entered into the matrix. |
| Crew Survival Method (CSM) | Program integrated hazard analyses must identify 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 (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 cross-referenced to documentation or analysis that verifies the adequacy of the survival method identified. |
| Background | Beginning at PDR, document the chronology of major events associated with the hazard, including related flight history, tests, and any significant failure summaries that drove design/operation changes, etc. Include a summary of any failure history or other anomalous events associated with the hazard cause. Include information which |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 16 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

| | |
|--|--|
| <p>adds understanding to the hazard, changes to the hazard, supporting documentation, etc. Include a summary of safety related requirements which were evaluated for completeness and adequacy associated with the hazard. Include a description of any hazard causes that were initially identified but then eliminated along with a brief summary of the rationale used to eliminate the cause from the report. Include a description of the current design configuration that reflects the current analysis as well as a description of any design changes made since the last report delivery.</p> | |
| The following data elements shall be documented in the hazard report for each hazard cause. | |
| 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. 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, moderate, low, or very low as defined in Table 4-2. |
| 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. When available, qualitative failure history should be consulted when determining the likelihood. The time parameter for assessing the likelihood is for the life of the program. Update the rationale and classification at each design milestone review based upon the evaluation of the successful implementation of the control and verification strategy. |
| Severity | The severity level is an assessment of the worst-case effects of the hazard assuming controls are not 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 4-3). 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 reduce 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. Provide a summary statement of any actual operational constraint, when applicable. Include a description of all the necessary design/operational controls for this hazard cause, including references to the technical requirements (e.g., factors of safety, design standards) necessary to ensure the control is implemented, including documentation references, if applicable. To the extent practical, the hazard report should include pointers with unique identification(s) to specific controls documented in the retention rationale for the |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 17 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

| | |
|----------------------------|---|
| | <p>applicable CILs in order to minimize duplication. The hazard controls shall 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.</p> |
| Failure Mode(s) | <p>Provide a reference list of any applicable failure modes that result in the hazard cause as documented in the Element FMEA. This list should refer to the specific FMEA section(s) and applicable mission phase(s) pertaining to each cause, and contain a brief descriptor for each reference. Reference(s) should not point to the entire FMEA for each such item. If there are no applicable failure modes documented in the FMEA, provide the following statement: "No direct linkage from the FMEA to this hazard cause has been identified at this time."</p> |
| Verifications | <p>Provide a summary with sufficient detail/explanation of the verification methods (testing, inspection, analysis, etc.) which ensure 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 ensure consistency between the hazards and the CILs. The 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 (by PDR) and control (by 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:</p> <ul style="list-style-type: none"> • PDR – Identify and document the specific verification type (i.e., test, analysis, inspection, or demonstration) applicable to each hazard control as well as a description of the planned verification activities which outline the overall verification strategy providing enough detail to facilitate an evaluation of test and verification planning for effective hazard controls. • CDR – Completion of document number or completion plan with estimated completion date (ECD) of verification activities to ensure the effectiveness of each hazard control is identified and required for the CDR delivery. • DCR – Document completed hazard control verifications, including reference to specific documents (test reports, analysis reports, etc.) where control verification is demonstrated. A verification tracking log (VTL) or other traceability tool shall cross-reference each verification to an approved Element/Program document to assure effective implementation of the controls. |
| Verification Status | <p>Identify the status of each verification as either closed or transferred to a VTL that includes an estimated completion date.</p> |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 18 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

3.1.4 System Safety Analysis Report

This report, one developed by each Element and one developed by the Program, shall be delivered separately or as a combined deliverable with the hazard reports to the Program and Elements in conjunction with the PDR, CDR, and DCR milestone reviews. An initial draft plan of the hazard analysis approach is delivered first at SDR or 90 days after contract initiation. The remaining data elements of the SSAR are required beginning at PDR. Engineering data needed to understand the system is welcome but not required to be delivered with the report; however, all resource data are required to be referenced. The system safety analysis report shall contain the following:

- **Hazard Analysis Approach** – Document the methodology used to perform the hazard analysis and the method of evaluating against required criteria. Document and provide a summary of the method(s) used to ensure all hazards have been identified. The hardware, software, operations, maintenance, facilities, and environments including GSE and GFE for each phase of the program life cycle are considered in the analysis. Provide any analysis tool(s) (i.e., fault trees, fish bone, or other logic diagrams) used to perform the hazard analysis and a summary of the methods in which the tool(s) were used in the identification of hazards.
- **Ground Rules** – Document any ground rules made when conducting the analysis.
- **Hazard Analysis Results** – Provide a brief summary of each hazard that has been analyzed for the system. Reference the associated hazard report number. It is at the discretion of the Element as to whether the hazard reports would be an appendix to the SSAR or a separate document. Document the results in a hazard risk matrix where each report risk is scored for its likelihood of occurrence and severity. Each report risk should be assigned equal to the highest combined likelihood and severity assigned to a single cause within that report. Enter each hazard report number into the corresponding likelihood and severity block according to the risk assigned to that report hazard. In the event that the highest combined likelihood and severity risk is equal for two separate causes within the report, place the report number in both corresponding blocks.
- **Integrated Hazard Summary** – Apart from the hazards identified above, if this system impacts any integrated hazards, those should be described here.
- **Operational Control Summary** – Identify and document which hazards utilize operational controls or personal protective equipment (PPE), what those controls are, and the rationale for utilizing an operational control rather than another option in the hazard reduction precedence sequence.
- **Waiver Summary** – Document any waivers to applicable Program or Element requirements with special attention to any anticipated or previously approved noncompliance reports (waivers to safety requirements) for the system.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 19 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

- **Failure History – Safety Impact Summary** – If this system has been modified in response to any previous failures or anomalies, document a summary of those failures here. Provide detailed information on any failure/anomaly resolutions that have changed any hazard controls, or investigations which have uncovered new failure modes or hazard causes.
- **Hazard Development History** – Include all hazards and hazard causes that were initially identified then later eliminated from the analysis, and the rationale behind the elimination.
- **Abort Triggers** – Identify and define the operating parameters for each abort trigger and trace the corresponding hazard(s) to the applicable abort trigger documented in the abort conditions report SLS-SPEC-<**TBD-009**>. (This data element applies to the Program Integrated Hazard Analysis only.)

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 20 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

4.0 HAZARD ANALYSIS DATA DELIVERY REQUIREMENTS

The SLS Program shall deliver a hazard analysis consisting of a system safety analysis report and hazard reports derived from performing a program integrated hazard analysis per Section 3.1.2 and a cross-program integrated hazard analysis per Section 3.1.3 as defined in Table 3-1.

The SLS Program Elements shall deliver, as defined in Table 4-1, a hazard analysis consisting of a system safety analysis report and hazard reports derived from performing an element hazard analysis per Section 3.1.1.

Table 4-1. Hazard Analysis Delivery Schedule

| Hazard Analysis Data Element | SDR ¹ | PDR | CDR | DCR |
|--|------------------|-----|-----|-----|
| System Safety Analysis Report (per Section 3.1.4) | • | • | • | • |
| Hazard Reports: | | | | |
| • Hazard Report Number | • | • | • | • |
| • Hazard Title | • | • | • | • |
| • Report Status | | • | • | • |
| • Mission Phases | • | • | • | • |
| • Mission Effectivity | | | | • |
| • Hazardous Condition Description | • | • | • | • |
| • Hazard Cause Summary | • | • | • | • |
| • Acceptance Rationale | | • | • | • |
| • Fault Tolerance to the Hazard | | • | • | • |
| • Hazard Risk Matrix (See Figure 4-1) | | • | • | • |
| • Crew Survival Method (Program Only) | | • | • | • |
| • Background | | • | • | • |
| • Hazard Causes (document the items below for each cause) | • | • | • | • |
| o Cause Title | • | • | • | • |
| o Cause Description | • | • | • | • |
| o Likelihood of Occurrence | | • | • | • |
| o Likelihood Justification | | • | • | • |
| o Severity | • | • | • | • |
| o Controls | | • | • | • |
| o Applicable Failure Modes (Element only) | | • | • | • |
| o Verifications | | • | • | • |
| o Verification(s) Status | | | | • |
| ¹ A “•” indicates required delivery of documentation for the data element row at the milestone at the head of the column. | | | | |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 21 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

4.1 Hazard Analysis Review Process Requirements

In accordance with NPR 8715.3, NASA General Safety Program Requirements, a safety review process will be used to assist SLS in ensuring that the SLS safety analyses are compliant with applicable requirements, comprehensive, technically accurate, and that residual risks are at acceptable levels. This SLS safety review process shall be conducted in conjunction with the Program/Element milestones.

Between milestone reviews, the Elements will provide SLS Program with read-only access to hazard report and system safety analysis report working data in the contractor's native data systems in accordance with the contract statement of work. The SLS Program and Elements shall support the review process outlined in this section.

4.1.1 SLS Hazard Analysis Review Process Overview

The hazard review process for the SLS Program will include a review of the hazard analysis by personnel independent of those that developed the product. SLS hazard analyses shall be dropped as reviewable documents during Program/Element milestone reviews. At each milestone review, a summary of the hazard analysis will be presented to the Milestone Review Board. The presentation provided to the Milestone Review Board focuses on the hazard reports which identify the most significant risks. The presentation may include the control and verification strategy for the hazard causes, the resulting safety risk, and the identified level of failure tolerance (including identifying if any waivers will be required). The Program hazard review process is defined in the following sections.

4.1.2 Element Hazard Analysis Review

Each Element will perform a hazard analysis. The hazard analysis will be evaluated for compliance to requirements and to assess the overall technical risk. The hazard analyses will be submitted for review at each Element milestone review. At each Element milestone review, the Milestone Review Board shall be presented with a summary of the safety analysis, which documents the residual safety risks. The focused safety review of the S&MA analyses presented to the Milestone Review Board includes the S&MA analyses (Hazard Analysis, Probabilistic Risk Assessment, etc.) which identify the most significant safety risks. The presentation may include the control and verification strategy for the hazard causes, the resulting safety risk, and the identified level of failure tolerance (including identifying if any waivers will be required). Any high risks or technical concerns that are identified outside of the milestone review process are to be communicated to the Element CSO. The CSO will ensure that unresolved technical issues are presented to the appropriate Program/Element-level Board for resolution.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 22 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

4.1.3 Program Integrated Hazard Analysis Review

The SLS Program will perform an IHA. The IHA will be delivered to the SLS Safety Assurance Team (SAT) and evaluated for compliance to requirements and to assess the overall technical risk (see SLS S&MA Plan for details on the hazard analysis review process roles and responsibilities). The IHA will be submitted for review at each Program milestone review starting at SRR. At each Program milestone review, the Milestone Review Board shall be presented with a summary of the safety analysis, which documents the residual safety risks. The focused safety review of the S&MA analyses presented to the Milestone Review Board includes the S&MA analyses (Hazard Analysis, Probabilistic Risk Assessment, etc.) which identify the most significant safety risks. The presentation may include the control and verification strategy for the hazard causes, the resulting safety risk, and the identified level of failure tolerance (including identifying if any waivers will be required).

Any high risks or technical concerns that are identified outside of the milestone review process are to be communicated to the Program CSO. The CSO will ensure that unresolved technical issues are presented to the appropriate Program/Element-level Board for resolution.

4.1.4 Other In-House Safety Analysis Review (e.g., Payload Adaptor)

Each Element that has in-house work will perform a safety analysis (e.g., hazard analysis, failure modes and effects analysis). The safety analyses will be delivered to the SAT and evaluated for compliance to requirements and to assess the overall technical risk (see the SLS S&MA Plan for details on the hazard analysis review process roles and responsibilities). The safety analyses will be submitted for review at each Element milestone review. At each Program/Element milestone review, the Milestone Review Board shall be presented with a summary of the safety analyses, which documents the residual safety risks. The focused safety review of the S&MA analyses presented to the Milestone Review Board includes the S&MA analyses (Hazard Analysis, Probabilistic Risk Assessment, etc.) which identify the most significant safety risks. The presentation may include the control and verification strategy for the hazard causes, the resulting safety risk, and the identified level of failure tolerance (including identifying if any waivers will be required).

Any high risks or technical concerns that are identified outside of the milestone review process are to be communicated to the Element CSO. The CSO will ensure that unresolved technical issues are presented to the appropriate Program/Element-level Board for resolution.

4.1.5 In-Between Milestone Reviews

Since the hazard analyses are continually evolving/maturing throughout the life cycle, there is always the possibility that the hazard analyses will identify concerns which warrant management attention at any time. In addition, since some SLS hazard analyses will be performed “in-house,” this could allow the SAT access to in-house analyses more routinely than periodic milestone

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 23 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

reviews. In either case, any issues or concerns identified by these analyses and/or review of these analyses in-between milestone reviews should be brought to the attention of the CSO. This allows the CSO to determine the best path forward, which may include bringing issues of significance to the attention of SLS Boards (e.g., Chief Engineer’s Board (CEB), Program Control Board (PCB)/Element Control Board (ECB)) since these Boards have the authority to direct work and include the TAs.

4.2 Hazard Risk Acceptance and Approval Requirements

The NASA Programmatic Authority has the responsibility to formally accept residual safety risks with the concurrence of the TAs. Hazard reports are used as a mechanism to fulfill this responsibility and shall be presented to Program Management and the TAs for formal risk acceptance.

The level of management required to approve hazard reports and accept residual risk is determined by the risk level of the hazard. This strategy is applied to all hazard reports in SLS. The SLS risk acceptance strategy is depicted in Figure 4-1 with definitions to the data elements on the X and Y axes defined in Tables 4-2 and Table 4-3, respectively.

Note: Any hazard reports that identify that a waiver to the failure tolerance requirement may be required must be elevated to the Program Manager, Program CSO, and Program CE for approval, at a minimum.

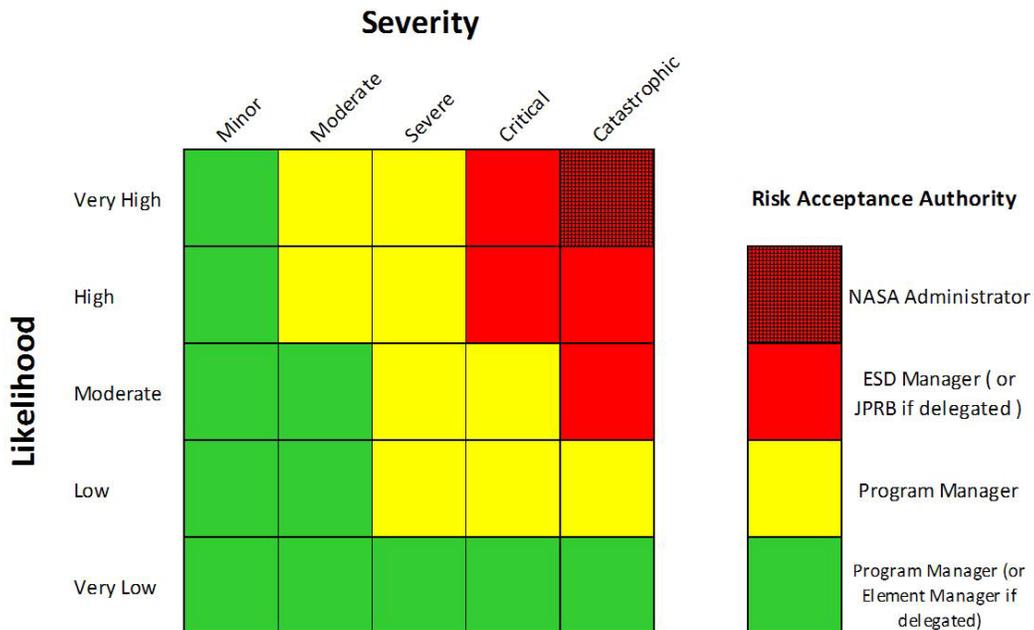


Figure 4-1. Delegated Hazard Risk Acceptance Matrix

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 24 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

Table 4-2. Hazard Likelihood Definitions

| Description | Hazard Likelihood Definitions |
|-------------|---|
| Very Low | Very unlikely to occur. Strong controls in place. |
| Low | Not likely to occur. Controls have minor limitations and/or uncertainties. |
| Moderate | May occur. Controls exist with some uncertainties. |
| High | Highly likely to occur. Controls have significant uncertainties. |
| Very High | Nearly certain to occur. Controls have severe limitations and/or uncertainties. |

Table 4-3. Hazard Severity Definitions

| Description | Hazard Severity Definitions |
|--------------|---|
| Minor | A. Minor injury not requiring first aid treatment, minor crew discomfort. B. Minor damage to nonessential flight assets. |
| Moderate | A. Injury requiring first aid treatment, moderate crew discomfort, or B. Major damage to nonessential flight assets. |
| Severe | A. Injury, illness, or incapacitation requiring emergency or hospital treatment, or B. Minor damage to flight or ground assets, or loss of nonessential flight assets. |
| Critical | A. Severe injury or occupational illness requiring extended hospital/medical treatment. B. Loss of mission or condition that requires safe haven. C. Major damage to flight or ground assets. |
| Catastrophic | A. Loss of life or permanent disabling injury. B. Loss of a facility or system critical to launch or flight operations. C. Loss of a launch vehicle prior to completing its primary mission. |

Note: These definitions have been approved to be applied across the three Programs (21st Century Ground Systems Program (21CGSP), SLS, & MPCV). However, the definition for Critical part B) may not apply in whole to the SLS Program.

Based on the delegated risk acceptance level in Figure 4-1, the hazard risk acceptance process will be as follows:

4.2.1 Controlled Risk (Green)

- Hazard Analysis shall be released on Change Request (CR) at DCR timeframe via the SLS CM Process.
- HA CR shall be reviewed at Chief Engineer Board for technical adequacy and risk acceptability.

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 25 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

- HA CR then flows through the Program/Element Control Board for approval and formal risk acceptance by the Programmatic Authority (Program/Element Manager).
 - Formal Risk concurrence is required by TAs (CE and CSO).

4.2.2 Accepted Risk (Yellow)

- Hazard Analysis shall be released on CR at DCR timeframe via the SLS CM Process.
- HA CR shall be reviewed at SLS Program Chief Engineer Control Board for technical adequacy and risk acceptability.
- HA CR then flows through the Program Control Board for approval and formal risk acceptance by the Programmatic Authority (Program Manager).
 - Formal Risk concurrence is required by TAs (CE and CSO).

4.2.3 Red Risk

- Hazard Analysis released on CR at DCR timeframe via Joint Program CM Process.
- HA CR shall be reviewed at Cross-Program Systems Integration (CSI) Panel Board for technical adequacy and risk acceptability.
- HA CR then flows through the Joint Program Control Board or ESD Control Board for approval and formal risk acceptance by the Program Managers or ESD Manager (Approval level defined in Cross-Program S&MA Plan).
 - Formal Risk concurrence is required by TAs (CE and CSO).

4.2.4 Top Right Box

- Hazard Analysis released on CR at DCR timeframe via Joint Program CM Process.
- HA CR shall be reviewed at CSI Panel Board for technical adequacy and risk acceptability.
- HA CR then flows through the Joint Program Control Board or ESD Control Board for approval.
- Hazard risk is elevated to the NASA Administrator for formal risk acceptance.
 - Formal Risk concurrence is required by TAs (CE and CSO).

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 26 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

4.3 Maintaining Hazard Reports Current

All changes shall be assessed for impact to the hazard analysis as part of the Element's and Program's change evaluation process. This is to ensure that potential hazards or hazard causes are not introduced or controls weakened without Program/Element approval. As part of the change package, an impact to baselined HRs will be identified along with acceptance rationale. Any potential increase in HR baselined risk shall be identified. A change shall be considered to involve an increase in baselined risk if any of the following is true:

- The change introduces a new hazard or new hazard cause(s). This includes changes to the FMEA/CIL that involve a new critical failure mode or critical failure cause that are incorporated to HR(s) via reference.
- The change eliminates or adversely affects previously defined hazard control or referenced CIL retention rationale.
- The change invalidates previously identified hazard control or referenced CIL retention rationale verification data (thermal/structural analyses, tests, etc.).
- The change reduces a margin of safety, even if the change still satisfies factor of safety requirements.
- For any other reason, the change increases probability of a hazard or critical failure mode manifesting itself; or increases the consequences of a previously identified hazard, hazard cause, failure mode, or failure cause.

4.4 Definitions

| | |
|--|--|
| Component | A combination of parts, devices, and structures, usually self-contained, which perform a distinctive function in the operation of the overall equipment. |
| Cross Program Integrated Hazard | Any hazard in which more than one program is a contributing cause, control, or verification for the hazard. |
| Effect(s) | The effect(s) describe the worst-case potential results on the program/element/subsystem and/or crew for each hazard cause occurrence prior to hazard control implementation. The FMEA/CIL end failure effects should be consulted when determining the effect(s). Also address any applicable local and intermediate effect(s). |
| Element | Physical entities within a program that have functional capabilities allocated to them necessary to satisfy mission objectives. Elements can perform all allocated system functions within a mission phase, or through mated |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 27 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

operations with other elements or programs (e.g., Multi-Purpose Crew Vehicle, Core Stage, Booster, Core Stage Engine, Avionics).

Emergency Operations

Operations (ground or flight) to prevent loss of life in the presence of imminent catastrophic conditions. Examples include fire extinguisher operations, as well as procedures necessary to support crew survival methods, such as abort, emergency egress, and escape.

Emergency Systems

Systems (ground or flight) that exist solely to prevent loss of life in the presence of imminent catastrophic conditions. Examples include the launch abort system (LAS), fire suppression systems, and crew escape systems.

Hazard

A condition, a state, an event, or an activity, internal or external to a system, which has the potential to cause harm.

Hazard Analysis

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

Operational Controls

Operational controls include both operational constraints as well as crew and support personnel training to prevent a hazard, lessen the likelihood or severity of a hazardous occurrence, or to mitigate its effects once it has occurred.

Permanent Disabling Injury

- An injury resulting in permanent impairment/disability of a critical part of the body,
- Exceedance of established human health limits (such as cumulative radiation levels) that has the potential for chronic life-threatening injury (such as cancer).

Subsystems

Physical entities within an element that have functional capabilities allocated to them necessary to satisfy mission objectives. Subsystems can perform all allocated functions within a mission phase, or through mated operations with other elements or subsystems (e.g., Guidance Navigation and Control, Avionics).

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 28 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

APPENDIX A ACRONYMS AND ABBREVIATIONS

| | |
|---------|---|
| 21CGSP | 21 st Century Ground Systems Program |
| ALERT | Acute Launch Emergency Restraint Tip |
| CAP | Corrective Action Plan |
| CDR | Critical Design Review |
| CE | Chief Engineer |
| CEB | Chief Engineer's Board |
| CIL | Critical Items List |
| CM | Configuration Management |
| CR | Change Request |
| CSI | Cross-Program Systems Integration |
| CSM | Crew Survival Method |
| CSO | Chief Safety and Mission Assurance Officer |
| CxP | Constellation Program |
| DCR | Design Certification Review |
| ECB | Element Control Board |
| ECD | Estimated Completion Date |
| EHA | Element Hazard Analysis |
| ESD | Exploration Systems Development |
| EVA | Extravehicular Activity |
| FAA | Federal Aviation Administration |
| FMEA | Failure Modes and Effects Analysis |
| FT | Failure Tolerance |
| FTA | Fault Tree Analysis |
| GFE | Government Furnished Equipment |
| GSE | Ground Support Equipment |
| HA | Hazard Analysis |
| HR | Hazard Report |
| IHA | Integrated Hazard Analysis |
| ISS | International Space Station |
| JPRB | Joint Program Review Board |
| LAS | Launch Abort System |
| MIL-STD | Military Standard |
| MPCV | Multi-Purpose Crew Vehicle |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 29 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

| | |
|---------|---|
| MSFC | Marshall Space Flight Center |
| NASA | National Aeronautics and Space Administration |
| NPR | NASA Procedural Requirements |
| NSTS | NASA Space Transportation System |
| O&SHA | Operating and Support Hazard Analysis |
| OPR | Office of Primary Responsibility |
| PCB | Program Control Board |
| PDR | Preliminary Design Review |
| PPE | Personal Protective Equipment |
| RQMT | Requirement |
| S&MA | Safety and Mission Assurance |
| SAE ARP | SAE Aerospace Recommended Practice |
| SAT | Safety Assurance Team |
| SDR | System Definition Review |
| SLS | Space Launch System |
| SPEC | Specification |
| SRR | System Requirements Review |
| SSAR | System Safety Analysis Report |
| TA | Technical Authority |
| TBD | To Be Determined |
| VTL | Verification Tracking Log |

| | |
|--|---------------------------|
| Space Launch System (SLS) Program/Project | |
| Revision: Baseline | Document No: SLS-RQMT-015 |
| Release Date: October 28, 2011 | Page: 30 of 30 |
| Title: SLS Program Hazards Analysis Requirements | |

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 sequentially numbered as applicable (i.e., <TBD-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-001 | 1.2 | Document number for ESD Cross Program S&MA Plan |
| TBD-004 | 2.1 | Document number for ESD Cross Program S&MA Plan |
| TBD-005 | 2.1 | Document number for SLS Abort Conditions Report |
| TBD-007 | 3.1.3 | Document number for ESD Cross Program S&MA Plan |
| TBD-009 | 3.1.4 | Document number for SLS Abort Conditions Report |