**SAR EXAMPLE**

The following document (SEAL-SSD-011) is provided as an example of possible layout for a Safety Assessment Report (Safety). Specific details on required content are included in AFSPCMAN 91-710 Volume 3, paragraph 2.5.3.10 and MIL-STD-882E, TAB 301. The Range User has the flexibility to decide on document layout and format.

As described in Volume 1, paragraph 2.5.3.10, the SAR provides a summary of the results of all hazards analyses performed IAW the requirements of the AFSPCMAN 91-710, as tailored and identify the program’s residual risk, if any. The SAR provides a comprehensive evaluation of the status of safety hazards and their associated risks prior to the test or operation of the system.

The SAR documents an assessment to identify the status, at the time of the report, of safety hazards, associated risks, mitigation measures, and formal risk acceptance decisions. This documentation includes the hazards that have been identified and eliminated, and specific procedural controls and precautions that are to be followed to mitigate the risks of hazards that could not be eliminated.

If the Range User chooses to use this template as a deliverable format, it is recommended that the Volume 3, paragraph 2.5.3.10 and MIL-STD-882E, TAB 301 be used as a checklist for populating the existing sections and subsections, or adding new sections or subsections to the document, as needed. This SAR example is by no means complete; therefore, the Range User should use the Volume 6, Section 4.3 as the driver for document completion.

[*Guidance:* S*ystems, subsystems, components, and processes covered by the hazards analysis and mitigations identified in this SAR are most likely discussed in detail in the MSPSP, GOP and FSDP. To ensure that there is no duplication of effort, if the sections within the SAR require system/subsystems information that is already covered in another deliverables document, then only a reference to that document and section is recommended. To facilitate cross-reference, provide document, section, and paragraph/table/figure reference.*]

[*Guidance: Note: Though the intent of this SAR is to be a standalone document, the focus on reducing duplication by referencing other program compliance documents, is encouraged. For specific sections, such as risk matrix discussions, details will be required to be included.*]

**<Company Name>**

DRAFT

**SAFETY ASSESSMENT REPORT**

**FOR THE**

**<Title> PROGRAM**

Document Number: XXXXX

Revision X, 15 Sep 2020

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

This document is only an example.

USSFMAN 91-710 Volume 1, Attachment 3, Paragraph A3.2.5.identifies detailed requirements regarding this report.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

<Company Name>

102 Maybury Gardens

Isle of Avalon, FL 32145

All identified hazards have been eliminated or controlled. The <Company Name> Corporation <Title> Program is considered ready for flight. Approval of this SAR report constitutes adherence to these statements.

Prepared by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

John Doe Date

<Company Name> System Safety Manager

Approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Adam Smith Date

<Company Name> Program Manager

**Document Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision****Identification** | **Revision****Date** | **Pages Affected** | **Change Description** |
| Initial Release | 18 Sep 19 | N/A | N/A |
| A | 21 Feb 20 | Appendix A  |  |
|  |  |  |  |
|  |  |  |  |

[*Guidance: The “change” section contains a summary of all changes to the latest edition of the SAR. All changes shall be highlighted using change bars or similar means of identification.*]

**Preface**

This document establishes and defines the <Company Name> Corporation Safety Assessment Report (SAR) and its elements as required by AFSPCMAN 91-710 [T] for the <Title> Program at Vandenberg AFB (VSFB).

<Company Name> Corporation, located at Isle of Avalon, Florida, has contracted with the USAF to launch <Title> launch vehicles from the Western Range. The <Title> launch vehicle consists of two stages. The first and second stage propellants are RP-1 and LOX.

**Table of Contents**

Glossary of Acronyms & Definitions

1 Introduction

1.1 Purpose and Scope

1.2 Reference Documents

1.3 Government Regulations

1.4 U.S. Space Force Requirements and Documents

1.5 Definitions and Terms

1.6 Abbreviations

2 System Assessment Overview

2.1 System description

2.1 System Safety Program Plan (SSPP)

2.2 Missile System Prelaunch Safety Package (MSPSP)

2.3 Ground Operations Plan (GOP)

2.4 Facility Safety Data Package (FSDP)

2.5 Operations Safety Plan (OSP)

2.6 Debris Recovery Plan (DRP)

3 System Safety Order of Precedence

3.1 Risk Assessment Process

3.2 Hazard Severity

3.3 Hazard Probability

3.4 Hazard Risk Assessment Matrix

3.5 Residual Risks

3.6 Hazard Tracking System

3.6 Software Safety Analysis

3.7 Hazard Verification

3.8 Hazard Verification Methods

3.9 Hazard Verification Status

4 System Safety Assessment

Appendix A Top-Level Hazards – Hazard Tracking System Summary

Appendix B Non-Compliance Documentation

# Glossary of Acronyms & Definitions

1. **Introduction**

This Safety Assessment Report (SAR) summarizes the results of all hazards analyses performed IAW the requirements of the AFSPCMAN 91-710 for the preparation, launch, and post launch activities of the <Company Name> Launch Operations at Vandenberg Space Force Base (VSFB), California.

* 1. **Purpose and Scope**
		1. Purpose

The purpose of the SAR is provide and document the comprehensive evaluation of the mishap risks associated with the <Company Name> <Program> and support the System Safety position of acceptable residual risk.

* + 1. Scope

This report has been developed in accordance with the requirements of AFSPCMAN 91-710 Volume 3, paragraph 2.5.3.10 and MIL-STD-882E, TAB 301. The SAR identifies all relevant safety features of the hardware, software, and system design. It also documents procedural, hardware and software related hazards that may be present in the <Program> system. Representative topics covered in this SAR include safety criteria/methodology, results of analyses, results of safety program efforts, identification of hazardous materials, system description, system operation, and conclusions/recommendations.

* 1. **Reference Documents**

[*Guidance: In this section, include all <Company Name> policies incorporated or referenced in this SAR. At a minimum, include documents that are referenced, such as the MSPSP, GOP, FSDP, SOP, Hazard Assessment Report, etc.*]

* 1. **Government Regulations**

MIL-STD-882E Department of Defense Standard Practice – System Safety

NASA-FTA-HBK Fault Tree Handbook with Aerospace Applications

NASA-STD-8719.7 Facility System Safety Guidebook

FAA System Safety Handbook, Chap 8: Safety Analysis/Hazard Tasks

* 1. **U.S. Space Force Requirements and Documents**

AFSPCMAN 91-710 Range Safety Requirements for the Eastern and Western Ranges as

tailored per launch program

* 1. **Definitions and Terms**
	2. **Abbreviations**
1. **System Assessment Overview**

The information contained in this SAR is current as of this release. SAR content is as follows:

This SAR provides an evaluation of the safety risks of the <Program> Program and is current as of this release. It systematically describes the system and any changes, identified potential hazard risks then traced to the top-level hazards and determined the risk assessment of those changes. This evaluation complies with the AFSPCMAN 91-710, MIL-STD-882E and the System Safety Program Plan. This SAR complies with the objectives stated in the SSPP ensuring adequate consideration is given to safety and the protection of personnel and resources.

This SAR summarizes the number of top-level hazards (TLH) along with their hazard risk indices (Ref. Table 3-3, Risk Index). Eight TLHs have a hazard severity level identified as “1 - Catastrophic” and four TLHs have a hazard severity level of “3 – Marginal”. However, all top-level hazards have a hazard probability level of “E - Improbable”. TLH are listed in Section 4, System Safety Assessment. TLH have all been mitigated to a MEDIUM level of risk, considered an acceptable level of residual risk for the program.

The sub-system hazards analysis (SSHA) has evaluated 82 specific hazards, with all but four mitigated to a LOW level of risk (Ref. Table 3-3). The remaining four have been mitigated to a MEDIUM level of risk, considered an acceptable level of residual risk for the program.

The operations for the program have developed 102 individual operating and support hazards assessment (O&SHA). All operations have been mitigated to a LOW level of risk.

The program has generated two requirements non-compliances (Ref. Table 4-2). One is an approved waiver for ESAD arming with less than the required number of inhibits. This waiver is driven by the AFSPCMAN 91-710 requirements and RCC-319, which requires arming the ESAD while the launch vehicle is still on the ground. The waiver will remain in effect for the life of the program. The second non-compliance is an approved Equivalent Level of Safety request that will be in effect through the first flight, pertaining to the implementation of 100% volumetric inspection on all vehicle pressure piping.

*[Guidance: Range User to identify their program’s TLHs, quantities, severity class and probability levels. Risk ranking may be based on individual Range User ranking system. MIL-ST-882E risk ranking is used in example.*]

The causal factors for each subsystem were analyzed, the hazard risk index for each causal factor was tallied, and the results entered into the hazard risk index matrix. The System Safety Hazard Analysis Report (XXXXX-X) details by worksheets, each causal factor for each subsystem and how it was eliminated, controlled, mitigated and verified to an acceptable level.

The hazards, safety deliverables, reports and processes mentioned herein are tracked and/or managed in order to maintain the safety of the <Program> Program and the payload system. Participation in review boards such as XXB, XXCB, and FXXB ensure design, procedures or process changes do not negatively impact the program or payload system.

The safety features, safety deliverables and safety analyses were summarized which provide the evidence that the effort to ensure the safety of the <Program> Program payload subsystems is acceptably safe. This document provides the overall safety risk assessment for the <Program> program. Based upon MIL-STD-882E, the risk is acceptable.

**2.1 System description**

System safety related information for the <Program> is captured in various documents required for missile system prelaunch safety approval. The following briefly discusses each document, which has been used to develop this SAR>

[*Guidance:* T*his section may be developed by referencing other program documentation such as SSPP, MSPSP, GOP, FSDP, etc.*]

**2.1 System Safety Program Plan (SSPP)**

Program technical and programmatic safety requirements are defined in the <Program> SSPP, <Program> AFSPCMAN 91-710[T] tailored requirements, and the contract applicable documents. These requirements along with other specific component derived requirements are incorporated into the component, system, and subsystem design specifications. The <Program> engineering elements are responsible for assuring design specifications are met in order to preclude hazards being generated by improper design. <Program> System Safety is responsible for ensuring the composite system meets the <Program> SSPP and contract safety requirements. Any design deficiency that generates a hazard not adequately controlled is identified and presented to the program for disposition as a Residual Risk. (See Reference 1.2.x.) The system safety process is discussed in Section 3.

**2.2 Missile System Prelaunch Safety Package (MSPSP)**

The Missile System Prelaunch Safety Package (MSPSP) provides a detailed description of all hazardous and safety critical ground support and flight hardware equipment, systems, and materials and their interfaces used in the launch of <Program>.

Specific items of interest are as follows:

* Hazardous material information
* Hazards analysis reports (XXXXX-X)
* Ground Support systems
* Non-ionizing energy
* ATP/QTP Reports
* NDE
* Ground software
* Inhibit Strategy/Fault Tolerance
* Etc.

[*Guidance: The specific item list should capture major items associated with MPSPS hazards, so as to allow the reader a point of reference if additional information is required.*]

**2.3 Ground Operations Plan (GOP)**

The GOP provides a detailed description of the hazardous and safety critical operations associated with a <Program> system and its associated ground support equipment.

Specific items of interest are as follows:

* Ground Operations
* Process flow timelines
* Training requirements
* Pressure vessles
* Ordnance
* Hazards Analysis reports (XXXXX-Y)
* O&SHA reports (XXXXX-Z)
* Etc.

[*Guidance: The specific item list should capture major items associated with GOP hazards, so as to allow the reader a point of reference if additional information is required.*]

**2.4 Facility Safety Data Package (FSDP)**

The FSDP provides a detailed description of the hazardous and critical systems of facilities and locations assessed as critical for the <Program>.

Specific items of interest are as follows:

* LPS
* Hazardous classification
* Back up power
* Emergency egress
* Aural/Visual Control Assembly
* Hazards Analysis reports (XXXXX-Q)
* Etc.

[*Guidance: The specific item list should capture major items associated with GOP hazards, so as to allow the reader a point of reference if additional information is required.*]

**2.5 Operations Safety Plan (OSP)**

The OSP provides a detailed description of all hazardous operating areas including launch complexes and associated areas and facilities for the <Program>. It is developed for unique, but frequently repeated, operations that require special or detailed safety considerations and clarifies and provides detailed safety requirements that are particular to the operating area or operation in question.

Specific items of interest are as follows:

* Emergency Evacuation Plans
* First Aid/Emergency
* General Emergency Procedures
* Personnel Accounting
* Lockout/Tagout
* Accident/Incident Reporting
* Etc.

[*Guidance: The specific item list should capture major items associated with GOP hazards, so as to allow the reader a point of reference if additional information is required.*]

**2.6 Debris Recovery Plan (DRP)**

The DRP provides a detailed description for the <Program> needed to address any inadvertent vehicle impact on land or near shore. This includes all prelaunch, launch, landing activities.

Specific items of interest are as follows:

* Initial Response
* System Safing
* Notification
* Debris Recovery
* Removal and Storage
* Etc.

[*Guidance: The specific item list should capture major items associated with GOP hazards, so as to allow the reader a point of reference if additional information is required.*]

1. **System Safety Order of Precedence**

The system safety process is a risk-management process and is described in detail in the <Program> SSPP, but can be summarized with the following steps:

* Identify risks using hazard analysis techniques as early as possible in the system life cycle.
* Develop options to eliminate, control, or avoid the hazards.
* Provide for timely resolution of hazards.
* Implement the best strategy.
* Control the hazard through closed-loop system

[*Guidance: Provide a brief description of risk-management process used in the SSPP. If the SSPP does not include a detailed discussion on risk-management, then include a detailed discussion here.*]

**3.1 Risk Assessment Process**

[*Guidance: Provide a description of risk assessment process used with references to is source (i.e. AFSPCMAN 91-710, MIL-STD-882E, etc.*]

The system safety precedence and risk assessment procedures used for the <Program> System Safety Program is based on MIL-STD-882E, System Safety. The risk assessment process determines the hazard severity, hazard probability and combines the severity and likelihood of occurrence into a Hazard Risk Assessment Matrix.

[*Guidance: The below hazard severity and probability levels can be copied from the Range User’s SSPP. They are required in this document for an understanding of Top-Level Mishap rankings and understanding of residual risk being presented in this SAR.*]

**3.2 Hazard Severity**

Hazard severity categories are provided to set a qualitative measure for the worst possible mishap as a result of personnel error, environmental condition; design inadequacy, procedural deficiency, or system, subsystem, or component failure or malfunction. Table 3-1 lists the definitions for the hazard severity categories established in MIL-STD-882.

**Table 3- 1 Hazard Severity Categories**

| **DESCRIPTION** | **SEVERITY CATEGORY** | **MISHAP RESULT CRITERIA** |
| --- | --- | --- |
| CATASTROPHIC | 1 | Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M. |
| CRITICAL | 2 | Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or monetary loss equal to or exceeding $1M but less than $10M. |
| MARGINAL | 3 | Could result in one or more of the following: injury or occupational illness resulting in one or more lost work day(s), reversible moderate environmental impact, or monetary loss equal to or exceeding $100K but less than $1M. |
| NEGLIGIBLE | 4 | Could result in one or more of the following: injury or occupational illness not resulting in a lost workday, minimal environmental impact, or monetary loss less than $100K. |

[*Guidance: The definitions may be tailored to specific company monetary thresholds based on Range User asset risk tolerance, but cannot be tailored based on injury or death.*]

**3.3 Hazard Probability**

The probability that a hazard will be created during the design life expectancy of the system is based on statistical probability data (Ref. XXXX) based on research analysis, and evaluation of historical safety data from similar systems. Table 3-2 reflects the qualitative hazard probability ranking used for <Program>.

[*Guidance: Provide a description of how hazard probability is determined. When available, the use of appropriate and representative quantitative data that defines frequency or rate of occurrence for the hazard is generally preferable to qualitative analysis*.]

**Table 3- 2 Hazard Probability Levels**

| **DESCRIPTION** | **LEVEL** | **SPECIFIC INDIVIDUAL ITEM** | **EXPECTED OCCURRENCE** |
| --- | --- | --- | --- |
| FREQUENT | A | Likely to occur frequently. | Continuously experienced |
| PROBABLE | B | Will occur several times in life of item. | Will occur frequently |
| OCCASIONAL | C | Likely to occur sometime in life of an item. | Will occur several times |
| REMOTE | D | Unlikely, but possible to occur in life of an item. | Unlikely, but reasonably can be expected to occur |
| IMPROBABLE | E | So unlikely, it can be assumed occurrence may not be experienced in the life of an item. | Unlikely to occur, but possible |
| ELIMINATED | F | Incapable of occurrence. This level is used when potential hazards are identified and later eliminated. | Incapable of occurrence. This level is used when potential hazards are identified and later eliminated. |

**3.4 Hazard Risk Assessment Matrix**

The combination of severity and probability are used to develop a hazard risk assessment matrix, as illustrated in Table 3-3. The matrix can prioritize the efforts of design engineers by identifying the hazards that are most critical to safe operation and maintenance of <Program>. Both design and safety engineers can focus attention and efforts on the most critical potential hazards in the configuration item design and eliminate or control those hazards as directed by the safety design process.

Each hazard receives a ranking of 1A through 4E, with 1A donating the highest Hazard Risk Index (HRI) (worst case) and 4E the lowest HRI (least hazardous). All hazards with an initial HRI of 1A, 1B, 1C, 1D, 2A, 2B, 2C, or 3A are considered HIGH risk and will be tracked until corrective action has reduced the hazard acceptable to the Ballistic Missile Defense Organization (BMDO) Director. All hazards with an initial HRI of 1E, 2D, 3B, 3C, or 4A are identified as MEDIUM risk and will be tracked until corrective action has reduced the hazard acceptable to Joint Program Office (JPO)-Program Manager (PM) approval. Hazards with an initial HRI of 2E, 3D, 3E, 4B, 4C, 4D, or 4E are deemed a LOW risk and will be tracked until reasonable mitigation actions are acceptable to GBI-PM approval.

**Table 3- 3 Hazard Risk Assessment Matrix**

| **FREQUENCY OF****OCCURRENCE** | HAZARD CATEGORIES |
| --- | --- |
| 1. Catastrophic  | 2. Critical | 3. Marginal  | 4. Negligible |
| A. FREQUENT | 1A | 2A | 3A | 4A |
| B. PROBABLE | 1B | 2B | 3B | 4B |
| C. OCCASIONAL | 1C | 2C | 3C | 4C |
| D. REMOTE | 1D | 2D | 3D | 4D |
| E. IMPROBABLE | 1E | 2E | 3E | 4E |
| F. ELIMINATED |  |  | Eliminated |  |
| **Hazard Risk Index** | **Risk Level** | **Risk Acceptance Authority** |
| 1A, 1B, 1C, 2A, 2B | **HIGH** | **Unacceptable:** Control or mitigation required to reduce risk level. |
| 1D, 2C, 2A, 3B | **SERIOUS** | **Undesirable:** <Program> Chief Operating Officer, or Vice President of Mission Assurance. |
| 1E, 2D, 2E, 3C, 3D, 3E, 4A, 4B | **MEDIUM** | **Acceptable:** Approval by Vice President of Mission Assurance, System Safety Manager, or Responsible Engineer |
| 4C, 4D, 4E | **LOW** | **Acceptable:** Approval Responsible Engineer |

[*Use the same level of approval required for Risk Acceptance as identified in the SSPP.*]

**3.5 Residual Risks**

If some hazards are mitigated to some degree but there is an element of uncertainty in the controls, the following options are available for the program management:

* Accept the risk, which is the most undesirable approach
* Prevent risk by switching to another technology or different procedure
* Control risk by eliminating the hazards of high priority.

[*Guidance: Discuss residual risks, referencing required approvals depending on risk level.*]

**3.6 Hazard Tracking System**

[*Guidance: Provide brief discussion of HTS. This section can be copied from the Range User’s SSPP.*]

The Hazard Tracking System (HTS) is an integrated <Program> system safety database and reporting system (AFSPCMAN 91-710 and MIL-STD-882E compliant HTS database). The <Program> maintains data for each identified hazard within the HTS. Information from this database is utilized to support System Level Program Reviews. All <Program> hazards will be entered into the HTS from any <Program> level source. The methodology, ground rules and assumptions followed in the <Program> Safety Analysis are summarized in the SSPP. HTS summary is included in Attachment A.

**3.6 Software Safety Analysis**

[*Guidance: Include discussion on software contributions to hazard risks.*]

Software can contribute to functional hazards by failing to perform a required task, performing non-required tasks, performing tasks out of sequence, or performing tasks for an incorrect duration of time. All <Program> systems and subsystems software functions are analyzed with respect to hazards that can be created by the computer hardware, software, human interaction, and input environmental factors. The software safety analysis is documented in Software Safety Hazard Analysis Report (SSHAR), Document XXXX-X.

The software criticality index risk assessment matrix is illustrated in Table 3-4.

**Table 3- 4 Software Risk Matrix**

|  |  |  |
| --- | --- | --- |
| **Software Criticality Index** (SwCI) | **Risk Level** | **Software Control Category and Risk Severity** |
| SwCI1 | HIGH | AT and Catastrophic/Critical, or SAT and Catastrophic. |
| SwCI2 | SERIOUS | SAT and Critical, or RTF and Catastrophic. |
| SwCI3 | MEDIUM | AT/SAT and Marginal, or RTF and Critical, or Influential and Catastrophic. |
| SwCI4 | LOW | Influential and Critical/Marginal/Negligable, or RTF and Marginal/Negligable, or AT/SAT and Negligable. |
| SwCI5 | Not Safety | No Safety Impact |

Notes: 1. Autonomous (AT)

2. Semi-Autonomous (SAT)

3. Redundant Fault Tolerant (RFT)

**3.7 Hazard Verification**

Hazard control verification is performed to assure that the stated hazard controls are implemented. Verifications for each hazard control are documented in the HTS and are closed out when the verification is complete. When all verifications in a Hazard Log are closed, the Hazard Log can be recommended for closure signifying that the hazard is adequately controlled and those controls are acceptable to the customer. The verification process defined in the following paragraphs will be adapted by the components.

[*Guidance: Provide a brief description of hazard verification used in the SSPP. If the SSPP does not include a detailed discussion on hazard verification, then include a detailed discussion here.*]

**3.8 Hazard Verification Methods**

[*Guidance: Provide a brief description of hazard verification methods. Include discussion of the HTS.*]

Hazard controls are verified by one or more of the methods listed below. The hazard analysis report must identify the specific nature of the verification method as documented in the appropriate hazard log in the web-based HTS.

1. Inspection. Verification of compliance with safety requirements by visual examination, without use of special laboratory equipment or procedures. This includes review of design drawings and operational procedures.
2. Analysis. Verification by a technical or mathematical evaluation that makes use of mathematical tools (e.g., models, algorithms or equations), charts, graphs, circuit diagrams, data reduction, and/or representative data.
3. Demonstration. Verification by exercising the applicable component under appropriate conditions to assess proper response. This method does not entail the recording of quantitative data except via checklists.
4. Test. Verification by exercising the applicable components under all appropriate conditions while using instrumentation to collect, record, analyze, and evaluate quantitative data.

**3.9 Hazard Verification Status**

[*Guidance: Provide a brief description of hazard verification status. i.e. Open, Recommended Closed, or Closed.*]

The status of each test, analysis, inspection, or demonstration is designated as Open, Recommended Closed, or Closed as defined:

* Open - Corrective action to eliminate or control the hazard has NOT been completed. The hazard will remain open even when the Program Manager (PM) accepts the hazard, pending completion of corrective action and verification.
* Recommended Closed – Corrective action to eliminate or control the hazard has been implemented and verified by the ESH Representative. The HTS is then recommended closed.
* Closed - Corrective action to eliminate or control the hazard has been implemented, verified and recommended closed by the ESH Representative. Closure of a hazard is based on the Safety Manager’s recommendation and is forwarded to the appropriate (PM) for concurrence. Vice-President will have final approval authority for the acceptance of high-risk hazards.

As verification activities are completed and as information becomes available, the status will be updated to include a summary assessment of the verification results; identification of the applicable test, analysis, or inspection report (by title and number); and the date on which the activity was satisfactorily completed. A hazard log is not considered "closed" until all hazard control verification activities (tests, analyses, inspections, demonstrations, etc.) identified on the log have been satisfactorily completed.

**4 System Safety Assessment**

The <Program> System Top Level Hazards (TLH) are listed in Table 4-1, along with their associated hazard risk indices. They comprise of eight TLHs have a hazard severity level identified as “1 - Catastrophic” and four TLHs have a hazard severity level of “3 – Marginal”. However, all top-level hazards have a hazard probability level of “E - Improbable”. Based upon MIL-STD-882E, the risk is acceptable and equates to a MEDIUM risk (Ref. Table 3-3), requiring approval by Vice President of Mission Assurance, System Safety Manager, or Responsible Engineer. TLH are included in Appendix A, as a sample of the HTS.

This level of residual risk for personnel will be further mitigated by operating under Pad Clear conditions, using automation, and late in launch count activation, and reduction of inhibits.

**Table 4-1** <Program> **Top Level Hazards (TLH)**

|  |  |  |  |
| --- | --- | --- | --- |
| **TLH ID**  | **TLH Title**  | **Hazard Severity** | **Probability of Occurrence** |
| xxxx.1 | Propellant System Leak or Rupture  | 1 | E |
| xxxx.2  | Pressurant System Leak or Rupture  | 1 | E |
| xxxx.3 | Cryogenic System Leak or Rupture  | 1 | E |
| xxxx.4  | Inadvertent Ignition of Ordnance  | 1 | E |
| xxxx.5  | Inadvertent Activation and/or Rupture of Battery  | 3 | E |
| xxxx.6  | Hazardous Materials  | 1 | E |
| xxxx.7 | Electrical Hazards  | 3 | E |
| xxxx.8 | Thermal Hazards  | 3 | E |
| xxxx.9  | Package, Handling, Storage and Transport Hazards  | 1 | E |
| xxxx.10  | RF Radiation Hazards  | 3 | E |
| xxxx.11  | Mechanical and/or Structural Failure  | 1 | E |
| xxxx.12  | Support Test/Ground Support Equipment Hazards  | 1 | E |

The sub-system hazards analysis (SSHA) has evaluated 82 specific hazards, with all but four mitigated to a LOW level of risk (Ref. Table 3-3). The remaining four have been mitigated to a MEDIUM level of risk, considered an acceptable level of residual risk for the program.

The operations for the program have developed 102 individual operating and support hazards assessment (O&SHA). All operations have been mitigated to a LOW level of risk.

For the ground processing software there are no software functions with a software criticality index of SwCl1 or SwCl2 and only three software functions classified as SwCl3 with a an associated MEDIUM level of risk (Ref. Table 3-4).

The sub-system hazards analysis (SSHA) has evaluated 22 specific hazards, with all but six mitigated to a LOW level of risk (Ref. Table 3-3). The remaining six have been mitigated to a MEDIUM level of risk, considered an acceptable level of residual risk for the program.

Table 4-2 lists requirements non-compliances details for the program. The current mission will proceed with one AFSPCMAN 91-710 driven waiver and one temporary (through first flight) equivalent level of safety (ELS) deviation associated with limitations on non-destructive examinations. Non-compliance documentation is included as Appendix B.

**Table 4-2** <Program> **Non-Compliance Data List**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Item** | **Tracking No.** | **Classification** | **Effectivity** | **AFSPCMAN 91-710 Reference** | **Description** | **Status** |
| 1 | <Prg>-SSE-20-01 | LAS/LCS | 1st Flight | Vol 3, 12.4.3.4 | Volumetric NDE requirements | Approved by ER/WR, info FAA |
| 2 | <Prg>-SSW-20-01 | PS | Life of program | Vol 3, Table 13.2 | ESAD arming and inhibits | Approved by ER/WR, info FAA |
| 3 |   |   |   |   |   |   |

**Notes:** 1. PS – Public Safety

 2. LAS – Launch Area Safety

 3. LCS – Launch Complex Safety

**Appendix A**

**Top-Level Hazards – Hazard Tracking System Summary**

|  |  |  |
| --- | --- | --- |
| **Hazard Report Number** | **HR-01** | **HR-02** |
| Name | Failure of Vehicle Primary/Secondary Structure | Inadvertent Release or Leakage of Propellant through a Mechanical Leak Path |
| Owner | E. Maiden | P. Diano |
| Status | Closed | Closed |
| Approval Date | 3/12/2020 | 2/9/2020 |
| Revision |   |   |
| Effectivity | Life of the Program | Life of program |
| Brief Hazard Description | Evaluates the risk of vehicle primary/secondary structure failure | Evaluates the risk of possible propellant lead |
| Risk Initial Severity | 3 | 3 |
| Risk Initial Probability | C | C |
| Risk Final Severity | 1 | 1 |
| Risk Final Probability | ESample | E |
| System/Subsystem/ Component Hazard Analysis Summary | Structrual loading, fatigue/corrosion, mfgr or assembly error assessed. | Valve, electrcial, or inadvertant command causes assessed. |
| Statement of Acceptable Level of Risk | Meets SSPP acceptable level of risk of medium or less, per XXX.XX | Meets SSPP acceptable level of risk of medium or less, per XXX.XX |
| Severity and Likelihood Justification |   |   |
| Fault Tolerance Statement | System contains fault tolerance design requirements per AFSPCMAN 91-710[T] Volume 3. | System contains fault tolerance design requirements per AFSPCMAN 91-710[T] Volume 3. |
| Number of Causes | 4 | 3 |
| Number of Controls | 13 | 7 |
| Number of Verificaitons | 16 | 13 |
| Open Verifications | 0 | 0 |
| Record of Relevant Engineering Changes | 0 | 0 |
| Requirement(s) Reference | AFSPCMAN 91-710V3, para xxxx.x | AFSPCMAN 91-710V3, para xxxx.x |
| Subcontractor Risk Data (as applicable) | N/A | N/A |
| Numerical Probability Assessment (if performed) | N/A | N/A |
| Preliminary Hazard Analysis Results (if performed) | N/A | N/A |

**Appendix B**

**Non-Compliance Documentation**



1. 