**SSHA & SHA EXAMPLE**

The following document (SEAL-SSD-013) is provided as an example of possible approach at developing and submitting both Sub-System Hazards Analysis and System Hazards Analysis. Specific details on required content are included in AFSPCMAN 91-710, Volume 1, A3.2.4.1 and A3.2.4.2 and Volume 3, paragraph 4.1. The Range User has the flexibility to decide on document layout and format.

As described in Volume 1, the SSHA and SHA shall identify and evaluate the safety considerations associated with components and equipment that could result in a hazard, including software functions (SSHA), and for the assessment of risk of total system design (including software), and specifically at subsystem interfaces (SHA).

If the Range User chooses to use this template as a deliverable format, it is recommended that the AFSPCMAN 91-710, Volume 1, A3.2.4.1 and A3.2.4.2 and Volume 3, paragraph 4.1 be used as a reference for populating the existing sections and subsections, or adding new sections or subsections to the document, as needed. This SSHA and SHA example is by no means complete; therefore the Range User should use the Volume 1 and Volume 3 as the driver for document completion.

**<Company Name>**

DRAFT

**SUBSYSTEM (or SYSTEM)**

**HAZARDS ANALYSIS**

**FOR THE**

**<Title> PROGRAM**

Document Number: XXXXX

Revision X, 15 Sep 2021

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

This document is meant as an example only. Detailed requirements

are included AFPSPCMAN 91-710 Vol 6, Attachment 2

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

<Company Name>

102 Maybury Gardens

Isle of Avalon, FL 32145

Prepared by:

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

John Doe

<Company Name> System Safety Manager

Approved by:

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

Adam Smith Date

<Company Name> Program Manager

**Document Change History:**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision **Identification** | RevisionDate | **Pages Affected** | **Change Description** |
| Initial Release | 18 Sep 20 | N/A | N/A |
| A | 15 Sep 21 | Appendix A | Updated Personnel Listing |
|  |  |  |  |

##### PREFACE

This document establishes and defines the <Company Name> Operating and Subsystem (or System) Hazard Analysis (SSHA, or SHA) and its elements as required by AFSPCMAN 91-710 [T] for the <Title> Program at Space Launch Delta 30 (SLD30).

<Company Name> Corporation, located at Isle of Avalon, Florida, has contracted with the USSF 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 AND DEFINITIONS

**1.0 INTRODUCTION**

**1.1** Purpose

**1.2** Scope

**1.3** Applicability

**1.4** SubSystem (or System) Hazard Analysis Updates

**2.0 METHODOLOGY**

**2.1** Risk Assessment

**2.2** Hazard Risk Severity

**2.3** Hazard Risk Probability

**2.4** Hazard Risk Assessment Code Matrix

**ATTACHMENT**

SSHA (or SHA) Analysis Worksheet

## GLOSSARY OF ACRONYMS AND DEFINITIONS

#### CFR Code of Federal Regulations

**GOP** Ground Operations Plan

#### GN2 Gaseous Nitrogen

#### Hazard Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of a system, equipment or property; or damage to the environment.

**Hazardous** Those operations classified as hazardous according to the

**Operations** following criteria: (1) consideration of the potential or kinetic energy involved, (2) changes such as pressure, temperature, and oxygen content in ambient environmental conditions, (3) presence of hazardous materials. Hazardous operations (including storage, transport, and handling) include, but are not limited to, the following: material (launch vehicle, payload, and other critical loads) handling operations; operations with acoustic hazards; operations with ionizing and non-ionizing sources and systems; operations with hazardous materials; pressure system (greater than 150) psig operations; propellant system operations; ordnance operations; and electrical system operations.

**LN2** Liquid Nitrogen

**LO2/LOX** Liquid Oxygen

#### Life cycle All phases of the system’s life including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal

**Mishap** An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

**Mishap Risk** An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence.

**OSHA** Occupational Safety and Health Administration

**Residual Mishap** The remaining mishap risk that exists after all mitigation

**Risk** techniques have been implemented or exhausted, in accordance with the system safety design order or preference.

**Risk Assessment** Hazard Assessment Code: An alphanumeric rating of hazard risk based

**Code (RAC)** upon its anticipated frequency of occurrence and the resultant severity of exposure to such risk.

**Safety** To have freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

**Safety Critical** An operation, process, facility, system, or component that controls or monitors equipment, operations, systems, or components to ensure personnel, launch area, and public safety (for example, Flight Termination System integrity); these operations, processes, facilities, systems, or components may or may not be hazardous in and of themselves.

**SSPP** System Safety Program Plan

**Subsystem** A grouping of items satisfying a logical group of functions within a particular system.

**System** An integrated composite of people, products, and processes that provide a capability to satisfy a need or objective.

**System Safety** The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time and cost, throughout all phases of the system life cycle.

**System Safety** An engineering discipline that employs specialized professional

**Engineering** knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated mishap risk.

**[T]** Tailored

# USSF United States Space Force1.0 INTRODUCTION

# 1.1 Purpose

The purpose of these SSHAs (or SHAs) is to evaluate activities for hazards and risks introduced into the system by components and equipment that could result in a hazard, including software functions (SSHA). [or, for the assessment of risk of total system design (including software), and specifically at subsystem interfaces (SHA)].

**1.2 Scope**

These SSHAs (or SHAs) identify and evaluate the safety considerations associated with design and functionality of components, subsystems and systems of the <Title> program and shall meet the intent of AFSPCMAN 91-710, Volume 1, A3.2.4.3 and Volume 6, A2.2.2.6.

# 1.3 Applicability

These SSHAs (or SHAs) are applicable to all hazardous system causes for the components and subsystems under consideration.

**1.4 Hazard Analysis Updates**

The applicable SSHAs (or SHAs) will be updated whenever there are any system design or functional changes to the <Title> Program. SSHAs (or SHAs) updates will follow the same approval protocol as the original documents.

# 2.0 METHODOLOGY

This analysis has been accomplished per the guidelines established in the applicable sections of AFSPCMAN 91-710 Range Safety Requirements as well as standard industry approach to systems engineering and hazard analysis methodology.

Once identified, each hazard is assessed in terms of its effect (i.e., its severity) should it be allowed to exist without the implementation of specific control measures.

Hazard elimination, control, or abatement measures/procedures are listed and/or described to ensure complete understanding of the risk management/risk reduction process employed.

The data have been analyzed, evaluated, formatted, and documented in compliance with Space Force and Industry Standards, including AFSPCMAN 91-710 Range Safety Requirements and MIL-STD-882E System Safety Program Requirements, where applicable.

As per AFSPCMAN 91-710, Volume 1, A3.2.4.1 and A3.2.4.2 and Volume 3, paragraph 4.1, these SSHAs (or SHAs) analyses shall identify components and functions that introduce *hazardous conditions.* While non-hazardous sequences will be routinely reviewed and assessed during the performance SSHAs (or SHAs), the specific results are not particularity noted herein.

For <Title> Program, the analysis task is conducted and documented in accordance with a flow process identified in the SSPP. The process:

1. Address SSPP requirements.
2. Where the item or process is explicitly covered in AFSPCMAN, the analysis and resolution process will consist of documenting compliance with the applicable requirements of that document. The results will be reflected in compliance matrices in the MSPSP.
3. Analysis is coordinated with the <Title> Program standard Requirements Compliance Verification process for determination of hazard status.
4. Results are approved for use by the <Title> Program System Safety Engineer.

**Exception:** Were a risk of a hazard exposure is created as a direct or indirect result of some specific action (or inaction) during non-hazardous steps, the details of each hazard as well as control measures will be assed in the reports.

# 2.1. RISK ASSESSMENT

In each case where hazards are identified, a Hazard Risk Assessment Code (RAC) has been assigned based on either the real or perceived degrees of hazard severity and occurrence probability. These codes have been developed using the severity and probability categories defined in MIL-STD-882 as reproduced in Table 2.2-1 and Table 2.3-1. The Risk Assessment Matrix defines and summarizes the risk acceptance criteria used for this analysis.

# 2.2. HAZARD RISK SEVERITY

MIL-STD-882 established system safety criteria guidelines to assist in the determination of hazard severity. The hazard severity categories are listed in **Table 2.2-1.** Hazard severity categories are defined to provide a qualitative measure of the most reasonable credible hazards resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction.

The effect of failure modes will be evaluated and categorized into one of the following severity categories:

## Table 2.2-1 Hazard Severity Categories

|  |  |  |
| --- | --- | --- |
| **DESCRIPTION** | **CATEGORY** | **EFFECT 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 work day, minimal environmental impact, or monetary loss less than $100K. |

# 2.3. HAZARD RISK PROBABILITY

The hazard probability levels listed in **Table** **2.3-1** represent the relative likelihood of occurrence of a mishap caused by the existence of an uncorrected or uncontrolled hazard.

## Table 2.3-1 Probability Levels

|  |  |  |  |
| --- | --- | --- | --- |
| **Probability Levels** | | | |
| **Description** | **Level** | Specific Individual Item | **Fleet or Inventory** |
| Frequent | A | Likely to occur often in the life of an item. | Continuously experienced |
| Probable | B | Will occur several times in the life of an item. | Will occur frequently |
| Occasional | C | Likely to occur sometime in the life of an item. | Will occur several times |
| Remote | D | Unlikely, but possible to occur in the life of an item. | Unlikely, but can reasonably 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. |

# 2.4 HAZARD RISK ASSESSMENT CODE MATRIX

The Hazard Risk Assessment Code (RAC) Matrix is shown in **Table 2.4-1.** This matrix categorizes total risk as a function of Severity and Probability.

## Table 2.4-1 Hazard Risk Assessment Code Matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Severity  Probability | **Catastrophic**  **(1)** | **Severe**  **(2)** | **Marginal**  **(3)** | **Negligible**  **(4)** |
| **Frequent**  **(A)** | **High** | **High** | **Serious** | **Medium** |
| **Probable**  **(B)** | **High** | **High** | **Serious** | **Medium** |
| **Occasional**  **(C)** | **High** | **Serious** | **Medium** | **Low** |
| **Remote**  **(D)** | **Serious** | **Medium** | **Medium** | **Low** |
| **Improbable**  **(E)** | **Medium** | **Medium** | **Medium** | **Low** |
| **Eliminated**  **(F)** | **Eliminated** | | | |

As stated in MIL-STD-882E, before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority as defined in the <Title> Program SSPP and agreed to by Range Safety. The system configuration and associated documentation that supports the formal risk acceptance decision shall be provided to the Range Safety for retention through the life of the system, or Program. The definitions in Tables 2.2-1 and 2.3-1, and the RACs in Table 2.4-1 shall be used to define the risks at the time of the acceptance decision. The <Title> Program shall be part of this process throughout the life-cycle of the system and shall provide formal concurrence before all Serious and High risk acceptance decisions.

Risk Acceptance Levels Criteria:

Unacceptable: High and Serious risk must be eliminated by design, or hazard severity/probability reduced to acceptable levels by imposition of external controls.

Waiver/Deviation: Waiver or deviation required. Acceptable only with full concurrence from upper management and customer and tracked to assure the controls in place do not change.

Acceptable: Acceptable with no further hazard tracking required. Operations permissible.

[*Guidance: Section 2.0 is partially reproduced from the organization’s SSPP and is used for PHAs, SSHAs, SHAs, and O&SHAs development. An alternative approach to developing deliverables for PHAs, SSHAs, SHAs, and O&SHAs is to produce a standalone document that encompasses Section 2.0 and is traceable to all developed PHAs, SSHAs, SHAs, and O&SHAs. This will limit the amount of duplicated text that needs to be attached to any individual PHAs, SSHAs, SHAs, and O&SHAs. Then the hazard analyses can be submitted as individual work sheets with individual tracking numbers. Reference* *SEAL-SSD-001.01, AFSPCMAN 91-710 Implementation Guide – Commentary.]*

|  |  |  |  |
| --- | --- | --- | --- |
| **Program** | **<Title>** | **Release Revision** |  |
| **System element** | **Hardware – Missile Structure** | **Approved Date** |  |
| **Mode** | **Ground Transport, Handling, and Integration, Range Operations** | **<Title> Program Approved** |  |
| **Hazard Location** | **Local Area Hazard** | **Analyst** |  |

|  |  |
| --- | --- |
| **References:** | 1. AFSPCMAN 91-710 Range Safety under Requirements Manual, Space Force Command Range Safety Policies and Procedures 2. <Title> Program System Safety Program Plan (SSPP) (XX-XXX) 3. Operations Safety Plan (XX-XXX) 4. Drawing No. XX-XXX |
| **Contributors / Reviewers:** |  |

This SSGA was developed in accordance with the <Title> Program System Safety Program Plan (SSPP), XX-XXX.

Summary Hazard Designations:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Case #** | **Description** | **Hazard Severity** | **Likelihood** | **Overall Ranking** | **Hazard Classification & Criticality** |
| SSHA-1 | Structural failure of unpressurized launch vehicle during lifting operations / Handling loads exceed the structural design limits | Catastrophic (1) | Improbable (E) | Medium | Launch Location Hazard |
| SSHA-2 | Structural failure of unpressurized launch vehicle during lifting operations / Operator caused impact, abrasion, or minor damage | Critical (2) | Remote (D) | Medium | Launch Location Hazard |

Sequence:

Figure:

[*Guidance: Where necessary for clarification, include a process sequence and/or sequence flow chart to help explain the SSHA.*]

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **HAZARD** | **SUBSYSTEM CAUSES** | **EFFECTS** | **MODE** | **SEV** | **PROB** | **IRAC** | **MITIGATIONS** | **SEV** | **PROB** | **FRAC** | **COMMENTS** | **STATUS** |
| SSHA-1 | Structural failure of unpressurized launch vehicle during lifting operations | Handling loads exceed the structural design limits | 1. Vehicle is dropped causing personnel injury or death, or loss of mission 2. Dropped high value component causing personnel injury, or result in mission impact | Ground Transport, Range Operations | 1 | D | Serious | 1. Unpressurized structures are designed to AFSPCMAN 91-710 requirements to a FS of 1.25x max transportation and handling loads, verified by analysis. 2. Unpressurized structures are qualification tested with a factor of safety greater than 1.25x max expected loads. 3. Handing crane and MHE designed and rated to greater than max expected vehicle/component loads. 4. Handling operations use qualified procedures reviewed, approved and performed by competent personnel. 5. Load lifting operations use load cells and other overload inhibits. 6. All MHE and riggings inspected prior to use and certified per AFSPCMAN 91-710 requirements. 7. Personnel have proper training and use proper PPE. | 1 | E | Medium |  | Open pending O&SHA and procedures |
| SSHA-2 | Structural failure of unpressurized launch vehicle during lifting operations | Operator caused impact, abrasion, or minor damage | 1. Damage resulting in failure of hardware and mission impact | Ground Handling, Integration, Transport, Range Operations | 2 | C | Serious | 1. Procedures in place to visually inspect structures for damage during all operations: prior to operation and also after operation.  2. Collision covers used where applicable on critical hardware items.  3. Personnel trained to avoid impacts or abrasions on structures.  4. Process in place to report any impact damage after inspection.  5. Lifting equipment designed to avoid adverse contact with structure.  6. Personnel use tethered tools when operating over the vehicle | 2 | D | Medium |  | Open pending O&SHA and procedures |

|  |  |  |  |
| --- | --- | --- | --- |
| **Program** | **<Title>** | **Release Revision** |  |
| **System element** | **FTS** | **Approved Date** |  |
| **TLM/SCF** | **Launch vehicle destruct function on the pad** | **<Title> Program Approved** |  |
| **Hazard Location** | **Launch Location Hazard** | **Analyst** |  |

|  |  |
| --- | --- |
| **References:** | 1. AFSPCMAN 91-710 Range Safety under Requirements Manual, Space Force Command Range Safety Policies and Procedures 2. <Title> Program System Safety Program Plan (SSPP) (XX-XXX) 3. Operations Safety Plan (XX-XXX) 4. Drawing No. XX-XXX 5. F |
| **Contributors / Reviewers:** |  |

This SSGA was developed in accordance with the <Title> Program System Safety Program Plan (SSPP), XX-XXX.

Summary Hazard Designations:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Case #** | **Description** | **Hazard Severity** | **Likelihood** | **Overall Ranking** | **Hazard Classification & Criticality** |
| SHA-1 | Launch vehicle destruct function on the pad / Inadvertent destruct signal is generated by erroneous radio link | Critical (2) | Improbable (E) | Medium | Launch Location Hazard |

Sequence:

1. [*Guidance: Description of the arming sequence and CONOPS supporting the SHA mitigations*.)

Figure:

1. [*Guidance: Figure showing ESAD arming functions in support of the sequence above and the SHA mitigations*.]

[*Guidance: Where necessary for clarification, include a process sequence and/or sequence flow chart to help explain the SHA.*]

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SHA No.** | **TLM/SCF** | **Hazard** | **System Causes** | **System Effects** | **Sev.** | **Prob.** | **IRAC** | **Mitigation** | **Sev.** | **Prob.** | **FRAC** | **Comments** | **Status** |
| SHA-1 | Launch vehicle destruct function on the pad | Inadvertent destruct signal is generated by erroneous radio link | Premature signal is sent for destruct | Inadvertent initiation of vehicle destruct system while on the pad | 2 | D | Medium | 1. FTS arming occurs in a Pad Clear condition with no personnel present. 2. ARM A and ARM B signals must be received prior to acknowledging. 3. Destruct signal has to be validated prior to initiation. 4. ESAD logic requires checks for appropriate arm sequence, or will error out. 5. Physical destruct button has flip cover preventing inadvertent pressing 6. FTS end-to-end testing vets system prior to launch operations. | 2 | E | Medium | Further procedural checks to be included in DOL procedure for radio link vetting | Open pending O&SHA and procedures |