**PHA / PHL Guidance**

The following document (SEAL-SSD-012) is provided as guidance document for the development of a Preliminary Hazards List (PHL) and a Preliminary Hazards Analysis (PHA). Specific details for performance and documentation are included in AFSPCMAN 91-710 Volume 1, Attachment 3, Task 3, paragraph A3.2.3 and MIL-STD-882E, TAB 201 and 202. Additional requirements are included in AFSPCMAN 91-710 Volume 3, paragraph 4.1. The Range User has the flexibility to decide on document layout and format.

As described in Volume 3, para 4.1, the Range User should submit the PHL prior to the commencement of the tailoring process prior to the system requirements review. Also, as described in Volume 1, paragraph A3.2.3, the Range User shall perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards and to identify requisite hazard controls and follow-on actions. The results of the PHA shall be submitted to Wing Safety at least 45 days prior to the cDR or equivalent program design activity. The results of the PHA shall be used as a guide for tailoring AFSPCMAN 91-710 for the program.

[*Guidance: This guidance document presents a very condensed approach to the development of both a PHL and PHA based on Hazard Analysis Techniques for System Safety, Clifton A. Ericson II, Wiley & Sons. 2005*. *It is highly recommended that Hazards Analysis Techniques for System Safety be thoroughly reviewed, as provides very clear and concise guidance to hazards analysis techniques, advantages/disadvantages, and common mistakes to avoid. Other sources may also be of value*.]

Fair Use Disclaimer: The information and content in this document are made available for educational and information purposes only. This document contains copyrighted material owned by a third party, the use of which has not been specifically authorized by the copyright owners. Notwithstanding a copyright owners’ rights under the Copyright Act, Section 107 of the Copyright Act allows limited use of the copyrighted material without requiring permission from the rights holders. For purposes such as education, criticism, comment, news reporting, teaching, scholarship, and research.

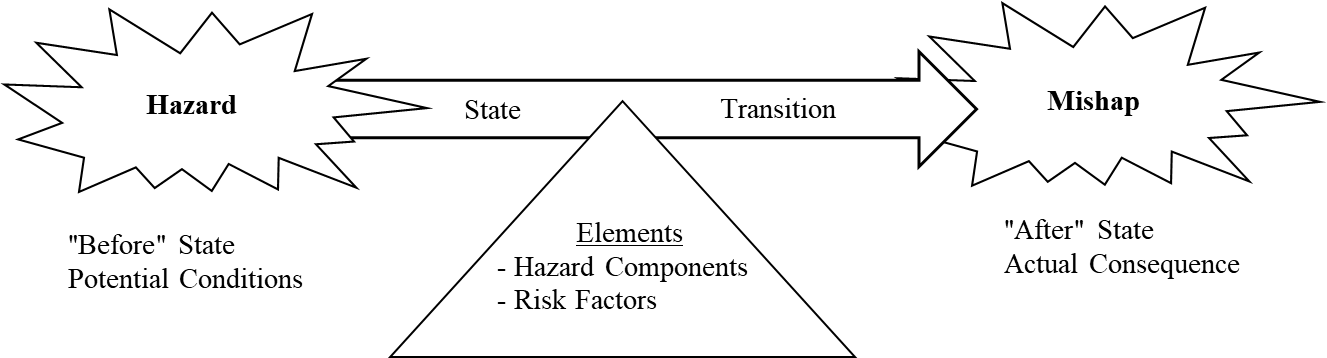
**Preliminary Hazards List**

The preliminary hazards list (PHL) documents potential hazards and causal factors for each hazard inherent in the system concept. Every hazard identified in the PHL will be subsequently analyzed with more detailed analysis techniques after the preliminary hazard analysis (PHA). MIL-STD-882E Task 201 provides guidance on the development of the PHL.

The purpose of the PHL is to identify and list potential system hazards applicable to any type of system(s) at a conceptual or preliminary stage of development. The PHL must be performed early in the development process and must include known or suspected hazards. It is recommended that the process be well structured to help ensure that all possible hazards are identified.

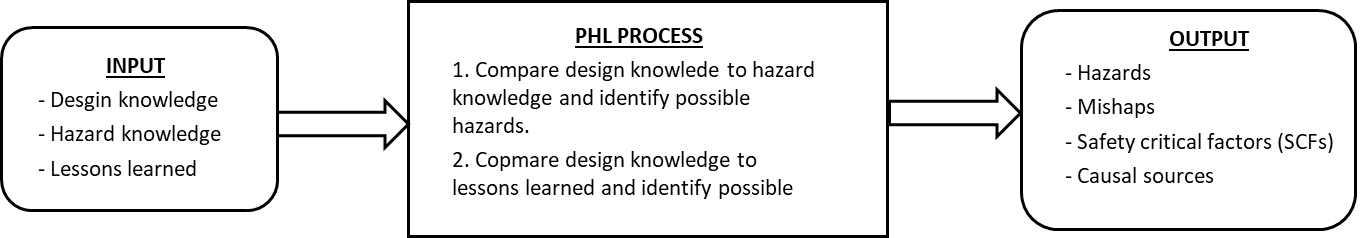
As an example, the PHL process should be based on the hazard-mishap relationship (Figure 1.) and evaluate design information in the form of the design concept, the operational concept, major components, planned for use in the system, major system functions, and software functions, amongst other considerations.

**Figure 1. Hazard-Mishap Relationship**



The following section provides brief guidance for the PHL development using Figures and Tables that provide guidance on the process and include some possible checklist for energy sources, general sources, and operational sources.

**Figure 2. Preliminary Hazard List Overview**



**Table 1. PHL Analysis Process**

|  |  |  |
| --- | --- | --- |
| **Step** | **Task** | **Description** |
| 1 | Define system | Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design, operation concepts, and major system components. |
| 2 | Plan PHL | Establish PHL goals, definitions, worksheets, schedule, and process. Identify system elements and functions to be analyzed. |
| 3 | Select team | Select all team members to participate in PHL and establish responsibilities. Utilize team member expertise from several different disciplines (e.g., design, test, manufacturing, etc.) |
| 4 | Acquire data | Acquire all of the necessary design, operational, and process data needed to for the analysis (e.g., equipment lists, functional diagrams, operational concepts, etc.) Acquire hazard checklists, lessons learned, and other hazard data applicable to the system. |
| 5 | Conduct PHL | 1. Construct list of hardware components and system functions. 2. Evaluate conceptual system hardware; compare with hazard checklists. 3. Evaluate system operation functions; compare with hazard checklist. 4. Identify and evaluate system energy sources to be used; compare with energy hazard checklist. 5. Evaluate system software functions; compare with hazard checklists. 6. Evaluate possible failure states. |
| 6 | Build hazard list | Develop list of identified and suspected system hazards and potential system mishaps. Identify SCFs and TLMs if possible from information available. |
| 7 | Recommend corrective action | Recommend safety guidelines and design safety methods that will eliminate or mitigate hazards. |
| 8 | Document PHL | Document entire PHL process and PHL worksheets in a PHL report. Include conclusions and recommendations. |

[*Guidance: The PHL is captured in item 8 of Table 1 above. The Range User may choose the format. As an alternative, the template document included in SEAL-SSD-013 for SHA and SSHA can be used. Attachments to this document also include generic PHL and PHA worksheets.*]

The typical hazard checklist used to conduct the PHL may include:

1. Energy sources
2. Hazardous functions
3. Hazardous operations
4. Hazardous component
5. Hazardous materials
6. Lessons learned from similar type system
7. Undesired mishaps
8. Failure mode and failure state considerations

As a reference, the AFSPCMAN 91-710 Vol 3 and Vol 6 catalogs safety requirements that have been developed based on historical lessons learned and whose chapters are divided on the bases of different hazard sources.

Tables 2 through 4 list possible additional hazard checklists.

**Table 2. Example of Possible Hazard Checklist for Energy Sources**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Fuels | 12 | Electrical generators |
| 2 | Propellants | 13 | RF energy sources |
| 3 | Initiators | 14 | Radioactive energy sources |
| 4 | Explosive charges | 15 | Falling objects |
| 5 | Charged electrical capacitors | 16 | Catapulted objects |
| 6 | Storage batteries | 17 | Heating devices |
| 7 | Static electrical charges | 18 | Pumps, blowers, fans |
| 8 | Pressure containers | 19 | Rotating machinery |
| 9 | Spring-loaded devises | 20 | Actuating devices |
| 10 | Suspension systems | 21 | Nuclear |
| 11 | Gas generators | 22 | Cryogenics |

**Table 3. Example of Possible Hazard Checklist for General Sources**

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | Acceleration | 11 | Oxidation |
| 2 | Contamination | 12 | Pressure |
| 3 | Corrosion |  | High |
| 4 | Chemical dissociation |  | Low |
| 5 | Electrical |  | Rapid change |
|  | Shock | 13 | Radiation |
|  | Thermal |  | Thermal |
|  | Inadvertent activation |  | Electromagnetic |
|  | Power source failure |  | Ionizing |
| 6 | Explosion |  | Ultraviolet |
| 7 | Fire | 14 | Chemical replacement |
| 8 | Heat and temperature | 15 | Shock (mechanical |
|  | High temperature | 16 | Stress concentrations |
|  | Low temperature | 17 | Stress reversal |
|  | Temperature variations | 18 | Structural damage or failure |
| 9 | Leakage | 19 | Toxicity |
| 10 | Moisture | 20 | vibration and noise |
|  | High humidity | 21 | Weather and environment |
|  | Low humidity | 22 | Gravity |

**Table 4. Example of Possible Hazard Checklist for General Operations**

|  |  |
| --- | --- |
| 1 | Welding |
| 2 | Cleaning |
| 3 | Extreme temperature operations |
| 4 | Extreme weight operations |
| 5 | Hoisting, handling, and assembly operations |
| 6 | Test chamber operation |
| 7 | Proof test of major component/subsystems/systems |
| 8 | Propellant loading/transfer/handling |
| 9 | High-energy pressurization/hydrostatic-pneumostatic testing |
| 10 | Nuclear component handling/checkout |
| 11 | Ordnance installation/checkout/test |
| 12 | Tanks entry/confined space entry |
| 13 | Transport and handling of end item |
| 14 | Manned vehicle tests |
| 15 | Static firing |

Lastly, a simple example is provided for the use of hypergolic propellants. If during the process of PHL development the analysis discovers that the system design will be using hypergolic propellant, then the analyst compares the hypergolic propellant to an appropriate hypergolic hazard checklist. From that hazard checklist it will be evident that hypergolic propellants are a hazardous element with the potential for toxicity/fire/explosion as a potential mishap. Different ignition sources for the hypergolic propellant will present many different hazards.

**Preliminary Hazards Assessment**

The PHA is the first level of analysis that determines the initial risk of identified hazards. The hazard mitigations determined through the analysis may become requirements for system design and operation. The starting point of the PHA is the PHL, as a collection of identified hazards. The PHA includes hazards, hazard causal factors, hazard mishap risk and controls that aim to mitigate hazards with unacceptable risk during the preliminary design phase of the system development.

For Range Operations, the review of the hazards and controls is the first review to be scheduled after program introduction (See SEAL-SSD-001 Attachment). These hazards and controls are then used in the tailoring of the AFSPCMAN 91-710.

The PHA should identify the majority of system hazards and affect the design for safety as early as possible in the development of the program. There are no alternatives to the PHA.

The development of the PHA analysis requires that the system safety analysis have a detailed understanding of three things:

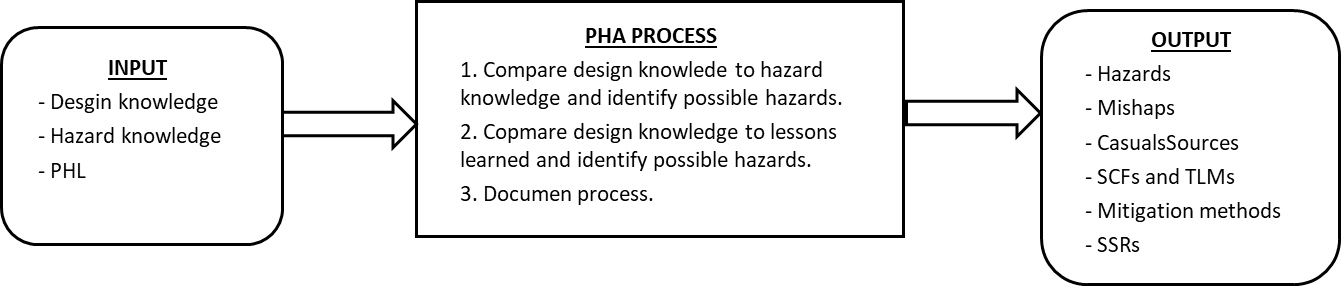
* Design knowledge: an understanding of the system design, including a list of major components.
* Hazard knowledge: an understanding about hazards, hazard sources, hazard components and hazards in similar systems. Primarily derived from hazard checklists and from lessons learned on the same or similar systems.
* The PHL.

Along with the PHL, the PHA can include top level mishaps (TLM).TLM is a significant mishap that can be caused by multiple different hazards, serving as a collection point for all the potential hazards that can result in the same outcome, but have different causal factors. An example of a TLM would be the explosion of a fully fueled launch vehicle on the pad. The sources of the mishap may be various (e.g. premature ordnance activation, propellant leakage, electrostatic discharge, etc.).

The results of the PHA will then be further evaluated as the system is decomposed and defined in the system hazard analysis (SHA), the subsystem hazard analysis (SSHA), and the operation and support hazard analysis (O&SHA).

The following section provides brief guidance for the PHA development using Figures and Tables that provide guidance on the process and include some possible checklist for energy sources, general sources, and operational sources.

**Figure 3. Preliminary Hazard Analysis Overview**

****

**Table 5. PHA Process**

|  |  |  |
| --- | --- | --- |
| **Step** | **Task** | **Description** |
| 1 | Define system | Define, scope, and bound the system. Define the mission, mission phases, and mission environments. Understand the system design, operation, and major system components. |
| 2 | Plan PHA | Establish PHA definitions, worksheets, schedule, and process. Identify system elements and functions to be analyzed. |
| 3 | Establish safety criteria | Identify applicable design safety criteria, safety precepts/principles, safety guidelines, and safety critical factors. |
| 4 | Acquire data | Acquire all of the necessary design, operational, and process data needed for the analysis (e.g., functional diagrams, drawings, operation concepts, etc.). Acquire hazards checklists, lessons learned, and other hazards data applicable to the system. Acquire all regulatory data and information that are applicable. |
| 5 | Conduct PHA | 1. Construct list of system items (e.g.) equipment, function, and energy sources for analysis. 2. Prepare a worksheet for each identified system item and its associated hazard.    1. Evaluate system hardware items against hazard checklists and TLMs.    2. Evaluate system operation functions against hazard checklists and TLMs.    3. Evaluate system energy sources against energy hazards checklists and TLMs.    4. Evaluate system software function against hazard checklists and TLMS.    5. Expand the list of items and hazards used in the analysis, if required.    6. Consider functional relationships, timing, and concurrent function when identifying hazards.    7. Utilize hazard/mishap lessons learned from other systems. |
| 6 | Evaluate risk | Identify the level of mishap risk present for each identified hazard before controls are implemented in the system design and operation. This evaluation of risk is commonly referred to as Risk Assessment and is captured through the Risk Assessment Code (RAC). |
| 7 | Document hazard controls | Document recommend controls to eliminate or mitigate identified hazards. Work with the design organization to translate the recommendations into design or operational requirements where appropriate. Also, identify existing controls the design or procedures that contribute to hazard mitigations.1 |
| 8 | Track hazards | Transfer newly identified hazards into the HTS. Update the HTS as hazards, hazard causal factors, and risk are identified in the PHA. |
| 9 | Document PHA | Document the entire PHA process and PHA worksheets in a PHA report. Include conclusions and recommendations. |
| 10 | Monitor hazard controls | Throughout the program lifecycle, the safety engineer will continue to monitor the implementation of, and effectiveness of, hazard controls to ensure that controls are effective in mitigating hazards as anticipated. |

**Note: 1.** Safety features such as inhibits within the design must at a minimum meet the requirements of AFSPCMAN 91-710 Volume 3, Chapter 3, General Design Policy and be coincident with Volume 1, para 3.3, Launch Area Safety.

[*Guidance: Deliverables requirements from AFSPCMAN 91-710 Volume 1 are captured in item 8 of Table 1 above. The Range User may choose the format. As an alternative, the template document included in SEAL-SSD-013 for SHA and SSHA can be used. Attachments to this document also include generic PHL and PHA worksheets.*]

The typical hazard checklist used to conduct the PHA is similar to that used for developing the PHL and may include:

1. Energy sources
2. Hazardous functions
3. Hazardous operations
4. Hazardous component
5. Hazardous materials
6. Lessons learned from similar type system
7. Undesired mishaps
8. Failure mode and failure state considerations

**RISK ASSESSMENT**

As referenced in Item 6 of Table 5, 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 6 and Table 7, below. The Risk Assessment Matrix defines and summarizes the risk acceptance criteria used for this analysis.

**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 5.** 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 6. 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. |

**HAZARD RISK PROBABILITY**

The hazard probability levels listed in **Table** **7** represent the relative likelihood of occurrence of a mishap caused by the existence of an uncorrected or uncontrolled hazard.

**Table 7. 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. |

**HAZARD RISK ASSESSMENT CODE MATRIX**

The Hazard Risk Assessment Code (RAC) Matrix is shown in **Table 8.** This matrix categorizes total risk as a function of Severity and Probability.

**Table 8. 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 Range User’s 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 6 and 7, and the RACs in Table 8 shall be used to define the risks at the time of the acceptance decision. The Range User’s 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: The Risk Assessment section is partially reproduced from the Range User organization’s SSPP and is used for PHAs, SSHAs, SHAs, and O&SHAs development.]*

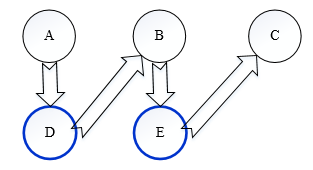
**PHA Commentary:** As noted previously, the majority of system hazards that affect the design for safety must be identified as early as possible in the development of the program to reduce the impact to the design. If not addressed early in the program this may cause redesign at a more mature design state, which would impact both cost and schedule.

The PHA’s intent is to identify the possible mishap hazards and provide a preliminary approach to mitigation and control. Further refinement to hazard mitigation will come from the Subsystem Hazard Analysis (SSHA) and the System Hazard Analysis (SHA)

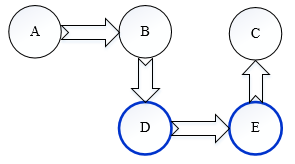
For example, if a system critical function, or a hazard is identified through the PHA that follows the sequence A → B → C,



and it is found to have an unacceptable corresponding Risk Hazard Index, or Risk Assessment Code, then through the process of the SSHA and the SHA, the minimum inhibit requirements of AFPSCMAN 91-710 Volume 3, Chapter 3 would be required to be incorporated. Say two inhibits for the purpose of this example, **D** and **E**. Therefore, a redesign of the process to include the two inhibits into the process would look like,



or



There have been many cases encountered for launch vehicle program development where the design has preceded the hazard analysis, leading to major redesigns at later stages of the program that result in major impacts to both cost and schedule. Early safety analysis then limits this risk.

ATTACHMENT A

SAMPLE PRELIMINAY HAZARD LIST WORKSHEETS

System Element Type:

| **No.** | **System Item** | **Hazard** | **Hazard Effect** | **Comments** |
| --- | --- | --- | --- | --- |
| PHL-1 | System A | Hazard 1 | Hazard Effect |  |
| PHL-2 | System A | Hazard 2 | Hazard Effect |  |
| PHL-3 | System B | Hazard 1 | Hazard Effect |  |
| PHL-4 | System B | Hazard 2 | Hazard Effect |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
|  |  |

Column Explanations/Notes

1. System Element Type: System under analysis (i.e. system hardware, system functions, system software, energy sources, etc.).
2. No. – hazard tracking number for the individual list item.
3. System Item – represents the sub-element of the system element type under consideration and represents the major system items of interest for this category (i.e. unpressurized structures, pressurized structures, GSE, ordnance, etc.).
4. Hazard – the specific hazard(s) that may result. This is the worst case scenario.
   1. Consideration should include whether it can it be reasonably assumed that a hazard can escalate to a catastrophic level without monitoring.
5. Hazard Effect – this is the resulting mishap and identifies the effect for the identified hazard. Effect results include such things as death, injury, damage, impact to system operation/mis-operation, etc.
6. Comments – records significant information for the development of the system item (assumptions, recommendations, SCFs, TLMs, system safety guidelines, etc.).

**Note:** One approach is that the system items be broken down into categories (i.e. hardware, software, energy source, system functions, etc.). As an example for the use of categories, using a hardware element type, the individual hazards are identified through analysis of the hardware element. Ordnance would be listed under hardware, as a possible hazard and its effects analyzed. Similarly, ordnance would again be listed under energy sources system element type. In the final PHL, there may exist some duplication, but this will allow for the identification of all ordnance-related hazards.

EXAMPLE PRELIMINAY HAZARD LIST WORKSHEETS

System Element Type: Hardware

| **No.** | **System Item** | **Hazard** | **Hazard Effect** | **Comments** |
| --- | --- | --- | --- | --- |
| PHL-1 | Launch vehicle  pressurized structures | Pressurized structure fails during handling operations | 1. Personnel injury, or death  2. GSE damage  3. Mission impact | Ground operations |
| PHL-2 | Launch vehicle  pressurized structures | Propellant tank over-pressurization | 1. Commodity leakage  2. Tank rupture  3. Personnel injury, or death  4. Environmental contamination | Ground operations |
| PHL-3 | Launch vehicle  unpressurized structures | Unpressurized structure fails during handling operations | 1. Personnel injury, or death  2. GSE damage  3. Mission impact | Ground operations |
| PHL-4 |  |  |  |  |
| PHL-X | Computer/Software fails to control propellant loading | 1. Propellant tank rupture  2. Propellant spill  3. Possible fire, or explosion | 1. Personnel injury  2. GSE damage  3. Launch vehicle damage  3. Mission impact  4. Environmental impact | Ground operations  Pad clear operation |

|  |  |
| --- | --- |
|  |  |

ATTACHMENT B

SAMPLE PRELIMINARY HAZARD ANALYSIS WORKSHEETS

|  |  |
| --- | --- |
|  |  |

System Element Type: Hardware

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PHA No.** | **Phase** | **Hazardous Description** | **Hazardous Effect** | **Sev.** | **Prob.** | **Initial RAC** | **Hazard Controls / Mitigation** | **Comments** |
| PHA-1 | Phase 1 | 1. Hazard 1 | 1. Hazardous Effect 1 | 2 | E | Medium | 1. Control 1  2. Control 2 | Comments |
| Phase 2 | 2. Hazard 2 | 1. Hazardous Effect 1  2. Hazardous Effect 2 | 2 | B | High | 1. Control 1  2. Control 2 | Comments |
| PHA-2 | Phase 1 | 1. Hazard 1 | 1. Hazardous Effect 1 | 3 | D | Medium | 1. Control 1  2. Control 2 | Comments |
| Phase 2 | 2. Hazard 2 | 1. Hazardous Effect 1 | 2 | E | Medium | 1. Control 1  2. Control 2 | Comments |

Column Explanations/Notes

1. PHA No: The specific Hazard Analysis reference number for the hazard. Ensures easy identification and tracking of hazards. PHA numbers may also be based on the phase within the CONOPS that helps further subdivide where the hazard is present (i.e. transport, MHE related, integration and test, etc.).
2. Phase: the phase within the CONOPS that helps further subdivide where the hazard is present (i.e. the phase column may be of help to further subdivide where in the process the hazard may be present.
3. Hazard description: Hazard detailed effects of failure to point of worst credible case scenario assuming no safeguards have been implemented.
   1. Purpose of evaluation without safeguards ensures that appropriate mitigations have been put in place to address hazard fully.
   2. Should identify initiating event, typically would identify specific equipment/failure mode.
4. Hazardous effect: – Worst potential final outcome (i.e. death, injury, resource damage, etc.).
5. Severity: Associated severity of the hazard as defined in MIL-STD-882E and the System Safety Program Plan.
6. Probability: Associated probability of occurrence of the hazard as defined in MIL-STD-882E and the System Safety Program Plan.
7. Initial Risk Assessment Code (RAC): Total Risk Assessment before implementation of controls. This corresponds to the hazard levels defined by the hazard severity and probability.
8. Hazard Mitigations/Controls: Actual safeguards or controls put in place that can/should independently reduce the potential probability or severity of the scenario. Examples:
   1. Redundant independent control valves reduce the potential for a catastrophic event by allowing a secondary control to prevent the scenario,
   2. PPE reduces the likelihood of exposure to personnel, but potentially does not prevent the scenario, ensure hazards are not missed, by recognizing partial protections.
   3. Pressure relief valves reduce impact from vessel rupture by allowing for release of pressure, however may introduce other hazards.
9. Comments: Place comments relating to values in the worksheet, such as design considerations addressing severity.

EXAMPLE PRELIMINAY HAZARD ANALYSIS WORKSHEETS

System Element Type: Hardware

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PHA No.** | **Phase** | **Hazardous Description** | **Hazardous Effect** | **Sev.** | **Prob.** | **Initial**  **RAC** | **Hazard Controls / Mitigation** | **Comments** |
| PHA-1 | Transport, unpressurized | Structural failure of launch vehicle | * Death, or injury to personnel * Major system damage * Mission impact | 1 | E | Medium | * Load bearing launch vehicle components designed to take into account ground handling and flight loads (static and dynamic) and the appropriate factors of safety. * Transport from Vehicle assembly site to launch site generally monitors transportation loads. | Range Operations |
| Pre-launch, unpressurized | * Structural flight components are load tested prior to use. |  |
| PHA-2 | Integration and test, unpressurized | Structural failure of material handling equipment | * Severe personnel injuries * Minor flight hardware damage | 2 | E | Medium | * Handling equipment will be designed, qualified, and maintained in accordance with AFSPCM 91-710 or more severe contract requirements. | MHE |
| PHA-3 | Integration and test, pressurized | Structural failure of material handling equipment. | * Death, or injury to personnel * Major flight hardware damage | 1 | E | Medium | * Handling equipment will be designed, qualified, and maintained in accordance with AFSPCM 91-710 or more severe contract requirements. | MHE |
| PHA-4 | Pre-launch, pressurized | Tip over of vehicle on launch stool due to: | * Loss of Launch vehicle. * Personnel injury or death. | 1 | D | Serious | * Vehicle held by clamps until minutes prior to launch | MHE |
| * Seismic Activity | * Analysis to verify seismic requirements |
| Post aborted launch, pressurized | * High Winds | * Pad clear condition when launch vehicle is pressurized |
| * Analysis to establish wind constraint placards will be performed. |
| PHA-X | Propellant load, pre-launch or WDR | Sw controlled over-pressurization of propellant tank(s) and rupture | * Personnel injury * GSE damage * Launch vehicle damage * Mission impact * Environmental impact | 2 | D | Medium | * SSSF shall be IV&V’d and include multiple Sw controls that prevent, alarm, and shut down propellant load | SSSF |

**Notes:** 1. PHA comments further separate system element type down to more specific function.

2. PHA items follow from the PHL list and expand the level of possible hazards that fall out of the PHL.

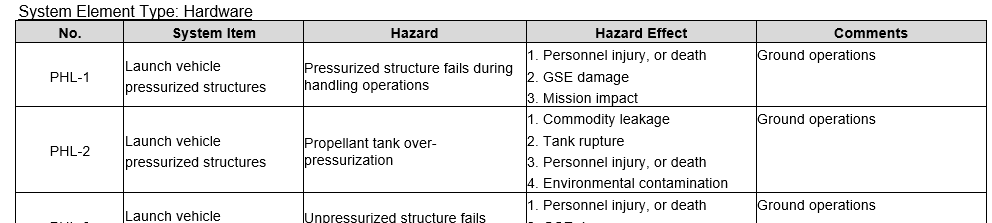
3. Note that Sw mitigations should not depend on mechanical inhibits. For the included example, the inhibits would be within the Sw logic and not, for example RV setting, prop tank FS, etc. These latter inhibits are still required, but are inhibits for the mechanical side of the hazard. The Sw hazard should rely on Sw mitigations.

ATTACHMENT C

SAMPLE PROGRESSION OF PHL, PHA, SSHA, O&SHA

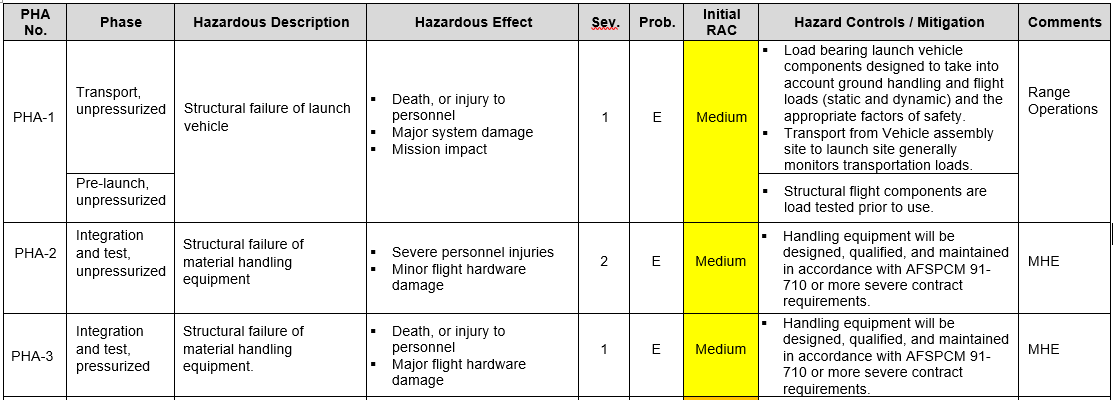
[*The below represent only one possible progression of PHL → PHA →SSHA → O&SHA. Actual hazard/safety analysis will determine the outcome*.]

**Sample PHL:**



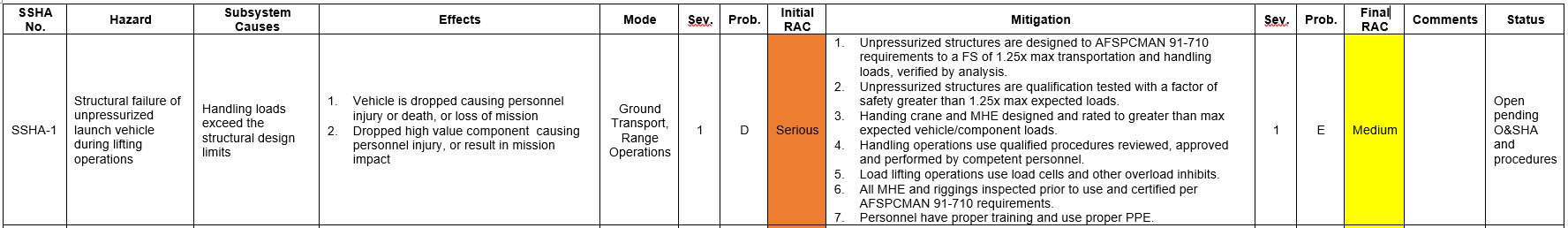
**Sample PHA:** PHL-1 is then expanded into PHA-1, -2, and -3.

System Element Type: Hardware – Missile structure



**Sample SSHA:** PHA-2 then becomes SSHA-2 and analyzed in more detail.

System Element Type: Hardware – Missile structure



**Sample O&SHA:** SSHA-1 mitigations 3 & 5 are further expanded n the O&SHA to just look at the crane braking system.

