DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-SOL-HL-V5.3
2. TITLE: Hazard LOG
3. DESCRIPTION AND INTENDED USE

The purpose of the Hazard Log (HL) is to provide a closed-loop hazard tracking system to record the identification, analysis, treatment and management of hazards and their associated risks. The HL provides a repository for the results of hazard analyses and acts as a source of evidence for the evaluation, reporting and, where applicable, certification of Materiel System safety.

The Contractor uses the HL, consistent with the scope of the Contract, to:

record and manage identified hazards to health, safety and the environment associated with the Materiel System;

provide a closed-loop record of the risks to health, safety and the environment associated with the identified hazards;

record the acceptance and follow-on actions to achieve Safety Outcomes; and

provide information for hazard analysis reports and inputs into Technical Data, including operator and Maintenance manuals and Training materials.

The Commonwealth uses the HL:

to understand the hazards and associated risks to health, safety and the environment associated with the Materiel System,

to review the Contractor’s controls for the identified risks;

to assist with evaluating whether or not the residual risk is acceptable; and

as input to any actions arising from the system safety program that need to be undertaken by the Commonwealth with regard to Materiel System implementation.

1. INTER-RELATIONSHIPS

The HL is subordinate to the following data items, where these data items are required under the Contract:

Systems Engineering Management Plan (SEMP);

System Safety Program Plan (SSPP);

Contractor Engineering Management Plan (CEMP); and

In-Service Materiel Safety Plan (IMSP).

The HL inter-relates with the following data items, where these data items are required under the Contract:

Project Management Plan (PMP);

Hazard Analysis Report (HAR);

Safety Case Report (SCR);

Materiel Safety Assessment (MSA);

Health and Safety Management Plan (HSMP);

design documentation; and

Failure Mode, Effects and Criticality Analysis Report (FMECAR).

1. APPLICABLE DOCUMENTS

The following documents form a part of this DID to the extent specified herein:

|  |  |
| --- | --- |
| 1. Nil |  |

1. PREPARATION INSTRUCTIONS
   1. Generic Format and Content

The data item shall comply with the general format, content and preparation instructions contained in the CDRL clause entitled ‘General Requirements for Data Items’.

The data item shall be based in electronic format acceptable to the Commonwealth (eg, a non-proprietary database), capable of producing outputs for a particular hazard analysis activity (eg, for a Preliminary Hazard Analysis), or each mishap risk and hazard in the HL, or other defined subset of the HL.

When the Contract has specified delivery of another data item that contains aspects of the required information, the data item shall summarise these aspects and refer to the other data item (including, for databases, the appropriate entry records or indices).

* 1. Specific Content
     1. Hazard Log Contents

The HL shall include the following information, as relevant to each mishap risk and hazard:

**Hazard Identification:** A unique hazard identification (index) number and brief description that identifies the hazard (eg, ‘unintended radiation emitted from radar set waveguide’).

**Hazard Description:** A detailed description of the potential/actual hazards inherent in the item being analysed, when resulting from normal or abnormal actions/ mishaps (eg, the hazards associated with the normal handling of a Problematic Substances as well as dealing with a spill of the Problematic Substances). The description is to identify the activities involving the hazard, the time periods, approximate frequency, and the number of personnel involved.

**Problematic Substances:** If hazards are associated with Problematic Substances, the following data shall also be recorded:

identification of the Problematic Substances, including the common or trade name, chemical name, chemical formula or ingredients, identifying stock numbers, physical form (solid, liquid, gas), current manufacturers, and suppliers;

location of the Problematic Substances within the Mission System and Support System Components;

quantity of the Problematic Substances within the Mission System and Support System Components, with traceability to version-specific hardware designs;

application, process, or activity whereby quantities of the Problematic Substances are embedded into the Mission System or Support System Components, or used during operations and support of the Mission System;

where a Problematic Substance is generated by the Materiel System, identify the circumstances under which generation occurs (eg, installation, test and evaluation, normal use, maintenance or repair of the system) and the quantity or rate of generation during operations and Maintenance;

reasonably anticipated quantities that may be discharged and the anticipated exposure rates during mishaps;

toxicity assessment, including a description of the expected frequency, duration, and amount of exposure (include the reference documentation, methods and calculations used to determine potency/toxicity assessment factors);

special control, training, handling measures, and Personal Protective Equipment (PPE) needed; and

reference to the applicable Safety Data Sheets (SDSs), which shall be prepared in accordance with DID-PM-HSE-SDS and delivered to the Commonwealth with the HL as supporting information.

**Problematic Sources:** If hazards are associated with Problematic Sources, the following data shall also be recorded:

identification of the Problematic Source, including the name of the item that is or that contains the Problematic Source, the kind of Problematic Source (controlled material or controlled apparatus), type (ie, ionising or non-ionising radiation source) and the frequency or particle nature of the radiation, as applicable;

location of the Problematic Source within the Mission System and Support System Components;

the intended purpose and function of the Problematic Source;

for Problematic Sources that are controlled materials, the element or chemical name and symbol of the nuclide and its atomic mass, physical form (ie, solid, liquid or gas), chemical form (eg, organic compound), activity (in Becquerel), half life, recommended working life; and

for Problematic Sources that are controlled apparatus, the operating parameters (eg, nominal and peak voltage), output parameters (eg, frequency range, wavelength, class), manufacturer and identification numbers, as applicable.

**Element Failure Mode(s):** Identify all element failure modes which can result in a hazard including human errors, single point and common mode failures. Include the effects of failures and events occurring in other subsystem elements, hazards arising from functional relationships between elements and the potential contribution of other subsystem (including those developed by other contractors/sources, off-the-shelf, non-developmental items, and GFE hardware or software) events, faults, and occurrences (such as improper timing). In the case of functional hazard analysis, consider modes which include the loss of function, degraded function or malfunction, or functioning out of time or out of sequence for the subsystems, components, and interfaces. Failure modes generally answer the question of ‘how’ it fails.

**Failure Propagation Mode(s):** Describe how the element failure mode can affect other elements, components, subsystems and systems. Identify the interfaces involved. In the case of functional hazard analysis, address functional interfaces in terms of connectivity and functional inputs and outputs. Consider the next effect in a possible mishap sequence until the final mishap outcome.

**System/Element:** Identify the system and element that this analysis is concerned with. For example, if a portion of the analysis applies to a particular subsystem, then identify the parent system and subsystem. In the case of a functional hazard analysis, indicate whether the function is expected to be implemented by hardware, software, or human control interfaces and, where known, identify implementing hardware or software components. Functions allocated to software should be mapped to the lowest level of technical design or configuration item prior to implementation.

**Applicability:** Identification of the version of specific hardware configurations of the system/subsystem or software releases, or Support System Component.

**Requirements references:** Identification details for documents that provide traceability to specifications, where applicable.

**System Event(s) Phase:** Describe the configuration or phase the system is in when the hazard is encountered; for example, during maintenance, during flight, during pre-flight, full-power applied, etc, or it could be encountered in all system events. Describe what is normally expected to occur as the result of operating the system/element during the system event phase.

**Causal factor:** Hardware, software, human, operational environment or other factors contributing to the creation of the hazard or the level of associated risk.

**Effect of Hazard:** Describe the detrimental (upstream and downstream) effects which could be inflicted on the subsystem, system, other equipment, facilities or personnel, resulting from this hazard.

**Hazard Indication:** Identify all warnings or other indications of the presence of the hazard to operational/maintenance personnel.

**Mishap:** Describe an event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

**Initial Risk Assessment:** Include an assessment of the risk associated with the hazard (classification of severity and probability of occurrence) and the resulting Hazard Risk Index. This is the assessment of the risk prior to taking any action to eliminate or control hazards and associated risks.

**Residual Risk Assessment:** Include an assessment of the residual risk associated with the hazard and the resulting Hazard Risk Index (HRI). This is the assessment of the risk after taking action to achieve Safety Outcomes.

**Event Risk Assessment:** Include an assessment of the risk associated with the hazard, and the resulting HRI, as it applies to a specified hardware/software configuration during an event. Typical events include developmental testing, operational testing, demonstrations, fielding, and post-fielding tests.

**Recommended Action:** Include risk mitigation measures (identified and selected with traceability to version specific hardware configurations or software releases) and recommended actions necessary to achieve Safety Outcomes. Sufficient technical detail is required in order to permit the Contractor and the Commonwealth to consult and adequately develop and assess criteria resulting from the analysis including the identification of:

changes needed in functional or design requirements for system hardware, software, facilities, tooling, or support/test equipment;

alternative designs and life cycle cost impact where appropriate. In the case of a functional hazard analysis, identify the requirements and constraints (to be included in the specifications) that, when successfully implemented, will achieve Safety Outcomes (eg, requirements for fault tolerance, detection, isolation, annunciation, or recovery);

required warnings, cautions, signage, supervision, access controls, safe work methods and special emergency procedures, including those to be included in operator, materials handling and maintenance manuals, and Training;

requirements for packaging, handling, storage, and transportation;

requirements for Personal Protective Equipment (PPE), where needed, and limitations for PPE use; and

any other information related to managing risks to health, safety and the environment.

**Status:** Provide the status of actions to implement the recommended, or other, hazard controls. The status shall include not only an indication of ‘open’ or ‘closed’ but also reference to the evidence, including applicable drawing(s), specification(s) and procedure(s), which support closure of the particular hazard.

**V&V method:** The V&V methods for risks and risk reduction following mitigation.

**Owner:** Person(s) and/or organisational element responsible for managing the particular hazard and its associated risks.

**Risk Acceptance:** Record of risk acceptance(s), including:

the Contractor’s risk acceptance authority by title and organisation, and date of acceptance;

the Commonwealth authority’s concurrence, as applicable, by title and organisation, and date of risk acceptance;

where applicable, the Approval by the Commonwealth Representative of a Problematic Substance or Problematic Source, within the applicable system or element; and

identification details for the signed risk acceptance document(s).

Note: Commonwealth ‘risk acceptance’ is not Acceptance. It acknowledges Commonwealth concurrence with the Contractor’s approach to minimising health, safety and Environmental risks. If a Problematic Substance or Problematic Source is the subject of risk acceptance, the HL records Commonwealth Approval of that Problematic Substance or Problematic Source, within the context of that risk.

**Hazard management log:** A record of the hazard entry and changes made to any part of the hazard record during the system's life-cycle.

**Remarks:** Include any other information relating to the hazard not covered elsewhere by this DID (eg, applicable documents, previous failure data on similar systems, or administrative directions).