DATA ITEM DESCRIPTION

1. DID NUMBER: DID-ENG-MGT-SSPP-V5.3
2. TITLE: SYSTEM SAFETY PROGRAM PLAN
3. DESCRIPTION AND INTENDED USE

The purpose of the System Safety Program Plan (SSPP) is to describe the tasks and activities for system-safety management and system-safety engineering that are required to achieve Safety Outcomes. The Approved SSPP provides a formal basis of co-ordination, consultation and understanding between the Contractor and the Commonwealth on how the system-safety program will be executed to meet contractual and legislative requirements.

The Contractor uses the SSPP to describe how the system-safety program will be accomplished to meet their legislative obligations and the Materiel Safety requirements included in the Contract.

The Commonwealth uses the SSPP to plan and monitor the Contractor’s system-safety program and to determine whether the program will achieve a level of Materiel Safety acceptable to the Commonwealth, and facilitate Commonwealth compliance with legislation, including the WHS Legislation.

1. INTER-RELATIONSHIPS

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

System Engineering Management Plan (SEMP); and

Integrated Support Plan (ISP).

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

Software Management Plan (SWMP);

Contract Master Schedule (CMS);

Hazard Analysis Report (HAR);

Hazard Log (HL);

Safety Case Report (SCR);

Materiel Safety Assessment;

Safety Data Sheets (SDSs);

the security-related data items required under the Contract (ie, in relation to the relationships between security considerations and safety considerations);

Quality Plan (QP);

Verification and Validation Plan (V&VP);

Verification Cross-Reference Matrix (VCRM); and

Health and Safety Management Plan (HSMP).

1. APPLICABLE DOCUMENTS

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

|  |  |
| --- | --- |
| MIL-STD-882E | *System Safety* |
|  | WHS Legislation |
|  | The system safety standards identified under the System Safety Program clause of the SOW |

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’.

When the Contract has specified delivery of another data item that contains aspects of the required information, the SSPP shall summarise these aspects and refer to the other data item.

The data item shall include a traceability matrix that defines how each specific content requirement, as contained in this DID, is addressed by sections within the data item.

* 1. Specific Content
     1. Program Scope and Objectives

The SSPP shall define a program to satisfy the system-safety requirements of the Contract by describing:

the scope of the system-safety program in terms of the system and the life-cycle phase;

the overall approach of the system-safety management, software safety management and engineering program to achieving Safety Outcomes, including through the hazard analyses required by clause 6.2.6 and related Contract requirements;

the integration of system-safety activities with the Systems Engineering and other functional elements of the Contract; and

the resource requirements needed to execute the SSPP.

The SSPP shall provide traceability for all contractually required system-safety tasks and responsibilities in a matrix that correlates the requirements of the Contract (including regulatory requirements and design constraints) to the location in the SSPP where each requirement is addressed by the system safety program.

* + 1. System Safety Interfaces

The SSPP shall describe the interfaces between the system-safety program and:

all other applicable safety disciplines including nuclear safety, range safety, explosive and ordnance safety, chemical and biological safety and laser safety;

Systems Engineering, and all other related disciplines including reliability and maintainability, Quality Management, software development, human factors engineering and medical support (for health hazard assessments); and

all system integration and test disciplines.

* + 1. System Safety Organisation

The SSPP shall:

describe the system-safety organisation or function within the Contractor’s organisation for the Contract, including the organisational and functional relationships and lines of communication;

identify the responsibility and authority of each person and organisational unit involved in executing each of the contractual system-safety requirements, including Key Persons, Subcontractors and system-safety groups;

describe the procedures that the Contractor will use to integrate system-safety and hazard management efforts for external system interfaces, including:

the roles of Commonwealth agencies, Associated Parties and Subcontractors necessary to integrate safety requirements for the total system;

the interfaces between the Contractor and each Subcontractor and Associated Party (eg, for integrating hazard analyses);

integrated product teams, or working groups, with representatives from Subcontractors and Associated Parties (as applicable);

any system-safety integration roles and their specific responsibilities for managing interfaces with external systems;

integrating hardware and software provided as GFE;

assigning requirements to organisational units and Subcontractors;

coordinating Subcontractor system-safety engineering efforts;

facilitating system-safety program reviews;

recommending mitigation measures including assessing feasibility, cost, and effectiveness of the measures, and allocating implementation responsibility to Subcontractors and Associated Parties;

reporting on program safety status and measures; and

the approach to consulting, coordinating and cooperating on safety issues, including between the parties, Subcontractors and Associated Parties; and

the process through which Contractor management decisions will be made, including timely notification to the Commonwealth of unacceptable risks, necessary actions in the event of mishaps, incidents, or malfunctions, and for requesting exemptions to system-safety requirements, program deviations and Engineering Change Proposals, when applicable.

* + 1. System Safety Program Milestones

The SSPP shall:

define a schedule of system-safety program milestones including required inputs and outputs, and start and completion dates;

relate the schedule of the system-safety program to system-level activities, Mandated System Reviews, and Milestones within the CMS;

identify the schedules for subsystem, component, and software safety activities applicable to the system-safety program but specified in other engineering studies and development efforts to preclude duplication; and

include a schedule of internal review meetings with Subcontractors and Associated Parties to cooperate, consult and coordinate the system-safety program effort.

* + 1. General System Safety Requirements and Criteria

The SSPP shall:

list the safety standards, system specifications, specified design constraints, and the civil and military regulations containing safety requirements that shall be complied with by the Contractor, including the Applicable Documents at clause 5 and identifying titles, dates and, where applicable, paragraph numbers;

describe general engineering requirements and design criteria for achieving safety outcomes applicable to design and development activities, including the role of Software in safety for each of the relevant states and modes);

identify safety requirements for all appropriate phases of the life cycle up to, and including, disposal;

describe the method for ensuring flow-down of hazard identification, mitigation strategies and associated system-safety program requirements to Subcontractors; and

describe the structure of the Materiel Safety baseline documentation to be delivered to the Commonwealth (ie, the SCR or Materiel Safety Assessment, as applicable to the Contract).

* + 1. Hazard Analysis

The SSPP shall describe:

the process for hazard identification, risk assessment, risk mitigation, communication of risks and support to risk acceptance including:

for hazard identification, the systematic identification process that evaluates the system throughout its life-cycle, including system hardware and software, system interfaces (including human interfaces), the intended use or application and operational environment, and disposal;

for risk assessment, the description of severity categories, probability levels, and the process for assigning Hazard Risk Indices (HRIs);

for risk mitigation, how decisions will be made within the system-safety process, with an emphasis on achieving Safety Outcomes including, in the context of cost to eliminate and minimise risks, whether the cost of further mitigation would be grossly disproportionate to the risk; and

for risk acceptance, the procedures for communicating and coordinating Commonwealth residual risk acceptance, including procedures for engaging the relevant Commonwealth authority(ies);

the approach for applying system-safety processes to extant system interfaces, subsystems or components (eg, for off-the-shelf items or legacy software) including the approach for verification and ensuring that existing data is consistent with the configuration, role and environment for the Mission System(s) and other Supplies;

the process for determining whether a qualitative or quantitative risk assessment is appropriate for a given hazard;

the hazard analyses to be performed (eg, preliminary hazard analysis, subsystem hazard analysis), the techniques to be used (eg, fault tree analysis, FMECA) and the documentation of the results, including the hazard analyses to be reported in each Hazard Analysis Report that is required to be delivered by the Contractor;

the scope of each analysis activity, the integration of Associated Party and Subcontractor hazard analyses within the overall system hazard analyses, and the depth within the system to which each analytical technique will be used;

for system interfaces, how analysis of the integrated system design, operations, and the interfaces between the products from each Subcontractor and Associated Party and the Mission System, or other major Supplies, will be executed;

the efforts to identify and control hazards associated with Problematic Substances and Problematic Sources incorporated within the design, and those Problematic Substances and Problematic Sources used in operation and support during the system’s life-cycle;

the efforts to identify and control WHS hazards directly related to the design (eg, noise, vibration, working at heights, working in confined spaces, lifting requirements and other human interface and ergonomic factors); and

the systematic software safety approach to be followed, when applicable.

The SSPP shall provide traceability to the hazard analysis tasks from MIL-STD-882E, or an equivalent standard acceptable to the Commonwealth Representative, and identify any tailoring of the standard tasks for the system-safety program under the Contract.

* + 1. System Safety Data

The SSPP shall:

describe the approach for collecting and processing pertinent hazard, mishap, and safety lessons learned data, including both historical data used to assist system safety analyses and current system data in the Hazard Log;

describe the management and use of the Hazard Log for recording each mishap risk and hazard, and the findings and results of the related analysis including hazard and safety-risk analyses, risk mitigation, and treatment;

identify all deliverable data items by title and number, and means of delivery (eg, hard copy, electronically); and

identify non-deliverable system-safety data and describe the procedures for accessibility by the Commonwealth and retention of data of historical value.

The SSPP shall, in accordance with clause 6.2.7.1, describe the scope of the SCR or Materiel Safety Assessment, as applicable to the Contract, and the supporting information to be delivered to the Commonwealth as evidence for the assessment of Materiel Safety.

* + 1. Safety Verification

The SSPP shall describe:

the Verification, and reporting, of the effectiveness of mitigation measures in achieving Safety Outcomes through test, analysis, inspection, or other means;

the Verification, and reporting, that hardware, software, and procedures comply with identified hazard management requirements;

requirements for certification, independent review evaluations and special testing of safety features (eg, insensitive munitions tests and render safe / emergency disposal procedures);

the procedures in place to transmit safety-related Verification information to the Commonwealth; and

the procedures for ensuring the safe conduct of all Verification activities.

* + 1. Audit Program

The SSPP shall describe the techniques and procedures to be employed by the Contractor to ensure that the objectives and related requirements of the system-safety program, including the achievement of Safety Outcomes, are being accomplished.

* + 1. Training

The SSPP shall describe the safety training for personnel involved with the system-safety program.

* + 1. Incident Reporting

The SSPP shall describe the incident alerting (including for mishaps and malfunctions), investigation and reporting processes, including notification of the Commonwealth.

* + 1. System Safety Working Group

Where the SOW requires the Contractor to establish a System Safety Working Group (SSWG), the SSPP shall include a plan for the SSWG, including:

objectives and the terms of reference for the SSWG;

the membership and points of contact for the SSWG; and

arrangements for the conduct of SSWG meetings.