Appendix X

System Safety Plan Template

This page is intentionally left blank.

Title Page
Document Control Panel
Table of Contents
List of Acronyms
Definitions

1. Overview

The System Safety Plan details the tasks and activities of system safety management and engineering. The plan defines a program to identify, evaluate, and reduce control hazards for a project or system, and its related equipment, facilities, material, services, personnel, and support. This plan describes the formal consideration given to implementation of system safety techniques during the life of the contract.

1.1 Scope

System safety is implemented to perform a rigorous and systematic evaluation of the hardware, facilities, and operations that fall under the contract. The plan identifies the system safety tasks and responsibilities necessary to support the project, including any facilities. The scope of the safety program should be identified here, including any overarching safety standards that apply.

1.2 System Safety Objective

The prime objective of the program is to provide the safest possible working environment. The primary tasks to achieve this objective are to eliminate hazards, or minimize and control hazards, to an acceptable level. Highlight the objectives in this section.

1.3 References

This section should include any project-specific reference documents, standards planned to be used, etc.

1.4 Definitions and Acronyms

Define any special terms used in the system safety program.

2. System Safety Administration

2.1 Organizational Structure Overview

Provide the project organization with emphasis on how safety engineering fits into the organization.

2.2 System Safety Organization

The system safety program is implemented by the system safety engineer, who should have a direct path to project manager. Provide an organizational chart showing system safety engineering and its relationship to the other ITS project organizations.

2.2.1 System Safety Engineering

The system safety engineer is responsible for the development, implementation, and maintenance of the system safety program. Establish how authority is given to the system safety engineer to act accordingly on safety issues. System safety engineering's responsibilities should be delineated and include:

- Developing, implementing, and maintaining the system safety program
- Identifying the safety requirements for implementation in the design
- Preparing hardware design checklists/guidelines, safety hazard analyses, and hard tracking data
- Providing project management with visibility of the safety program status, significant safety problems, and necessary improvements
- Participating in design reviews, working groups, and trade studies to adequately address hazards
- Reviewing and evaluating engineering drawings, changes, system diagrams, and system test procedures for hazards and compliance with safety standards
- Establishing and maintaining an interface with various project participants, including the ITS project members and component subcontractors
- Utilizing interfaces to comply with applicable safety requirements

- Coordinating system safety and safety test operations
- Inputting safety risk management information in the development process

2.3 System Safety Process

The system safety process is present throughout the development process. This section should illustrate that process and includes:

- How system safety engineering is involved with the design
-
- Participating in the ITS project design meetings
- Providing safety requirements, and developing safety guidelines and checklists
- Performing safety assessments
- Performing safety analyses
- Identifying and documenting hazards and the existing controls
- Documenting hazard risk reduction or elimination in the appropriate hazard analysis and in the hazard tracking system (HTS)
- Resolution of hazards will be made by the system safety working group (SSWG)

3. System Safety Overview

3.1 System Safety Milestones

This section describes the critical checkpoints for review of the system safety program, including:

- Defining and allocating requirements
- Preliminary design reviews (PDRs) and critical design reviews (CDRs)
- Installation and checkout (I&C)
- Integration and testing (I&T)
- Operations

3.2 Safety Task Schedule

This section provides a complete schedule of the entire system safety program showing detailed system safety tasks.

4. General Requirements and Criteria

4.1 Safety Approach and Standards

Safety criteria are developed from the program safety requirements, studies, hazard analyses, safety data, and experience. Sources include similar programs; industry standards and practices; government standards; specifications; and regulations. Safety criteria are utilized as the basis for the program's risk minimization. Safety technical requirements identified are incorporated into system design, hardware, operations, facilities, equipment, and procurement documentation. Safety criteria, standards, and requirements used as guidelines should be listed in this section.

4.2 Hazard Identification

Describe the hazard identification, including the variety of sources from which data is drawn, such as hazard analysis reports and contractor, subcontractor, and customer documentation. Hazard analysis requires documentation including system schematics; hardware designs; tool and support equipment designs; and schematics, manufacturing/assembly/test procedures, test memorandums and data, as well as related analyses dealing with failure modes, effects, and criticality analysis (FMECA); maintainability; and human factors and logistics support. The historical data provided by the project is used as a baseline in the identification and evaluation of hazards, and the potential effects on the project or system. How and when these data are provided to safety engineers should be defined. The hazard tracking process should be discussed, and the HTS detailed.

4.3 Severity, Probability, and Risk Assessment

During the analysis process, the system safety engineer evaluates each hazard for the severity of the worst possible consequence and the probability of the hazard occurring, and assesses the risk.

4.4 Hazard Closure Process

The process to identify and close a hazard should be described in this section. Also, this section should define the methodology used for the risk assessment process and the approval authority for accepting various levels of risk.

4.5 Engineering and Operational Changes

Formal interfaces between system safety and configuration management provide for safety review and analysis of configuration changes. The process should be explained here.

4.6 System Safety Precedence

To satisfy the safety requirements to resolve identified hazards, the following order of precedence is typically followed for eliminating hazards or reducing them to an acceptable level:

- Design to eliminate hazards
- Design for minimum hazard
- Incorporate protective safety design features or devices
- Provide warning devices
- Provide safety procedures and training
- Incorporate the use of personal protective equipment

5. Hazard Analysis

Hazard analyses, combined with the HTS, provide project management with hazard risk visibility and a monitoring method for hazard control implementation. System safety engineering performs hazard analyses and maintains the HTS. The purpose of the hazard analysis is to identify mishap potential; provide the basis for mishap risk assessment; and establish prevention criteria and operational constraints to eliminate or control mishap potential. This section should discuss the plans for hazard analyses.

5.1 Analysis Techniques

Safety analyses are the primary mechanism used for identifying and documenting the hazards associated with facilities, hardware, software, and operational environments. The choice of the types of hazard analyses used varies with the type of project and should be tailored to fit the project requirements and associated risk. The typical hazard analysis process includes:

- Preliminary hazard analysis (PHA)
- Installation hazard analysis (IHA)
- Subsystem hazard analysis (SSHA)
- System hazard analysis (SHA)
- Operations and support hazard analysis (O&SHA)
- Fault tree analysis (FTA)

Subsection paragraphs should be provided to describe each of the hazard analysis methods selected for the project.

5.2 Safety Assessment Report

The purpose of a safety assessment report (SAR) is to identify all system design safety features and to identify potential hazards that may be present in the system. The SAR will summarize:

- Safety criteria and methodologies used to classify and rank hazards, plus any assumptions on which the criteria or methodologies are based or derived, including the definition of acceptable risk as specified
- Results of analyses and tests performed to identify hazards inherent in the system
- Results of the safety program efforts
- List of all significant hazards
- Recommendations or precautions required for a safe environment
- List of any hazardous materials generated or used in the system

This section should describe the plans for and the schedule for the delivery of a SAR.

5.3 Subcontractor Safety Program Integration

Project team members are responsible for their own safety programs. Reporting on all safety issues, all hazards found by the subcontractors, resolution of hazards, etc., should be described in this section.

5.4 Hazard Tracking System

Identified hazards are documented in the HTS. This system will be used at all phases of the design, serving as the hazard documentation basis for the PHA, SSHA, SHA, and O&SHA. This section should describe the HTS, and how it will be used to document all identified hazards associated with hardware, software, waivers, deviations, or engineering changes. Describe how hazards will be opened, monitored, and closed using a closed-loop hazard tracking process.

6. Safety Data

The safety team will be required to pursue an aggressive program of acquiring current safety-related information and data. This includes studies, reports, and analyses of hazardous materials, processes, and conditions. Applicable federal standards and specifications, and industry consensus standards are maintained in current files. How system safety engineering will maintain all safety-related data generated on the project should be described in this section. The description may include:

- Data bank of system safety engineering data
- All safety documentation, hazard analysis reports, and the HTS data.

7. Safety Verification / Testing

This section should address the process to involve system safety engineering in the system test and demonstration process. It should describe how system safety engineering provides support to the test plan and procedure preparation as well as their involvement, if any, in actual testing.

8. Safety Training

The purpose of involving safety in the training process is to improve individual awareness of the working environment in order to identify and assist in eliminating hazards. How this is implemented on the project should be described here.

9. Mishap Investigation and Reporting

The mishap reporting and investigation policy should be established in this section.

10. System Safety Interfaces

System safety is an integral part of the total program effort and maintains both internal and external interfaces to identify and resolve hazards and avoid duplication of effort among the various program disciplines. The major safety engineering interfaces include:

- Customer interface
- Project office interface
- Systems engineering interface
- Hardware engineering interface
- Software engineering interface
- Human system interface (HSI)
- Reliability engineering interface
- Maintainability engineering interface
- Test engineering interface
- Logistics engineering interface
- Factory processes

Each of these, and any other project-peculiar interfaces should be described in subsections under this paragraph.

11. Acronyms and Notes

This section contains any general information that aids in understanding this document. This section will contain an alphabetical listing of all acronyms and abbreviations, along with their meanings as used in this document and a list of any terms and definitions needed to understand this document.