ORGANIZATIONAL MISSION ASSURANCE STANDARD: TIER 2

System Safety Program

SET ™

Revision: 1 Release: 01-30-2011 Effective: 01-30-2011

STANDARD

OBJECTIVE

This Standard defines *SET's* approach for implementing a System Safety Program. Through the interpretation and implementation of this Standard *SET* will tailor each system safety program to achieve safety requirements in a manner that is commensurate with the hazard severity level and life cycle phase of the product. At the time this Standard was written *SET* did not develop any ultra-high hazard severity level products, which require Capability Level 5 system safety activities. However, some Capability Level 5 activities are included in *SET's* Capability Level 4 System Safety Program Plan.

Note: Guidance for product hazard severity level determination is found in Figure 1.

APPLICABILITY

This Standard applies to all present and future *SET* sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors, regardless of whether a System Safety Program has been contractually imposed.

TABLE OF CONTENTS

FIGURES

TABLES

Note: The terms and acronyms used in this Standard are defined in Section 3.

1. INTRODUCTION

This Standard establishes the general requirements for a *SET* System Safety Program.

1.1 Scope

This Standard applies to all present and future *SET* sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors, regardless of whether a System Safety Program has been contractually imposed.

1.2 Purpose

Safety is the measure of the interaction of a product function with all other infrastructures, with or without a defined interface, to avoid accidents. Accidents are an unintentional intersection of dissimilar infrastructures, or like structures at somewhere other than the proper interface. System safety is the application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost. A system safety program is a set of interrelated processes that have the capability of assessing and eliminating or controlling existing and potential hazards. These include damage-threatening hazards, mission-impacting failures modes, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors. Through the interpretation and implementation of this Standard, *SET* will implement system safety programs that are tailored to achieve all pertinent system safety requirements in a manner that is commensurate with the hazard severity level and life cycle phase of the product. The generic product hazard severity level categorizations that apply to this Standard are shown in Figure 1.

Figure 1: Worst Case Hazard Severity Level Categories for Generic Products

Hazard Severity Level I	Hazard Severity Level I	Hazard Severity Level 1	Hazard Severity Level II	Hazard Severity Levels III & IV
• Defense satellites • Launch vehicles • Long-range missiles • Short-range missiles/rockets • Passenger aircraft / helicopters • Military aircraft / helicopters • Military drones / unmanned vehicles • Naval vessels • Nuclear weapons • Nuclear power plants • Cyclotrons	• Commercial / communications satellites • Fossil fuel / hydro-electric power plants • Oil tankers • Field / off shore oil rigs • Water filtration plants • Explosive devices • Passenger trains / buses • Cruise liners • Satellite ground control stations • Safety-critical hardware / software equipment / components • Safety-critical equipment testing/ monitoring apparatus • Life-saving medical equipment/device	• Science satellites • Cargo ships • Mobil / mechanized weapons • Freight trains • Amusement park rides • Elevators / escalators • Small private aircraft / helicopters • Automobiles / trucks / motorcycles • Farm equipment • Construction / demolition / excavation equipment • Factory machinery • Fire arms • Handheld construction / demolition / excavation equipment	• Industrial electronics • Motorized / manual hand tools • Mission-critical hardware / software equipment / components • Industrial computers / peripherals • Satellite communications relay stations • Laboratory / research equipment • Communications / utility equipment • Mission-critical equipment testing/ monitoring apparatus • Computer operating system software • Large Batteries	• Consumer electronics • Household appliances • Small Batteries • Battery operated toys • Infant/ children toys • Computer application program software • Personal computers / peripherals

The provisional AIAA Standard S-102.0.1 (Draft), *System Safety Program General Requirements*, partitions the system safety program into the following seven areas:

1. Authorization
2. Requirements Definition
3. Planning
4. Coordination
5. Engineering and Evaluation
6. Hazard Risk Assessment and Tracking
7. Requirements Verification

SET will implement the system safety program functional flow diagram shown in Figure 2 to progressively define and achieve system safety requirements and objectives throughout the product life cycle.

SET rephrases the descriptions of these system safety program areas in Table 1 in order to be more precise yet more generally applicable in context of the *SET* product line.

Table 1: System Safety Program Area Descriptions.

KEY SYSTEM SAFETY PROGRAM AREA	DESCRIPTION
Authorization	System safety program is appropriately empowered and resourced.
Requirements Definition	All system safety requirements are identified and correctly interpreted.
Planning	Selected activities are commensurate with budget, product hazard severity level, and life cycle phase.
Coordination	Safety-impacting activities performed outside of the system safety program are monitored and tracked.
Engineering & Evaluation	Industry acknowledged and cost-effective system safety engineering methods are applied across systems engineering.
Hazard Risk Assessment & Tracking	Residual hazard risk at time of delivery is commensurate with product hazard severity level
Requirements Verification	Compliance with each safety-critical and mission-critical requirement is actively verified

SET will implement the system safety program functional flow process shown in Figures 2 and 3 to progressively define and achieve system safety requirements and objectives throughout the product life cycle.

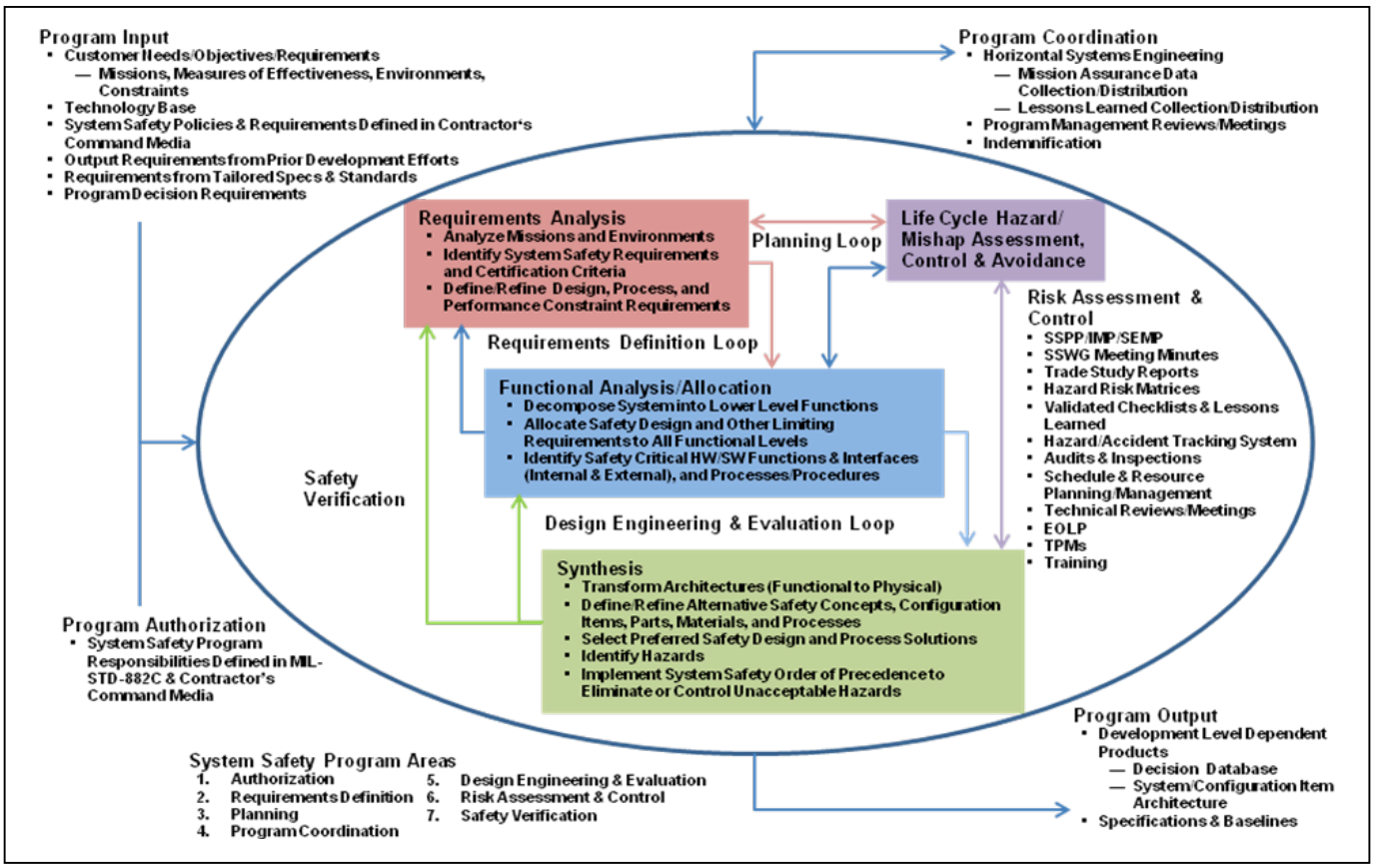

Figure 2: System Safety Program Functional Process Flow Diagram.

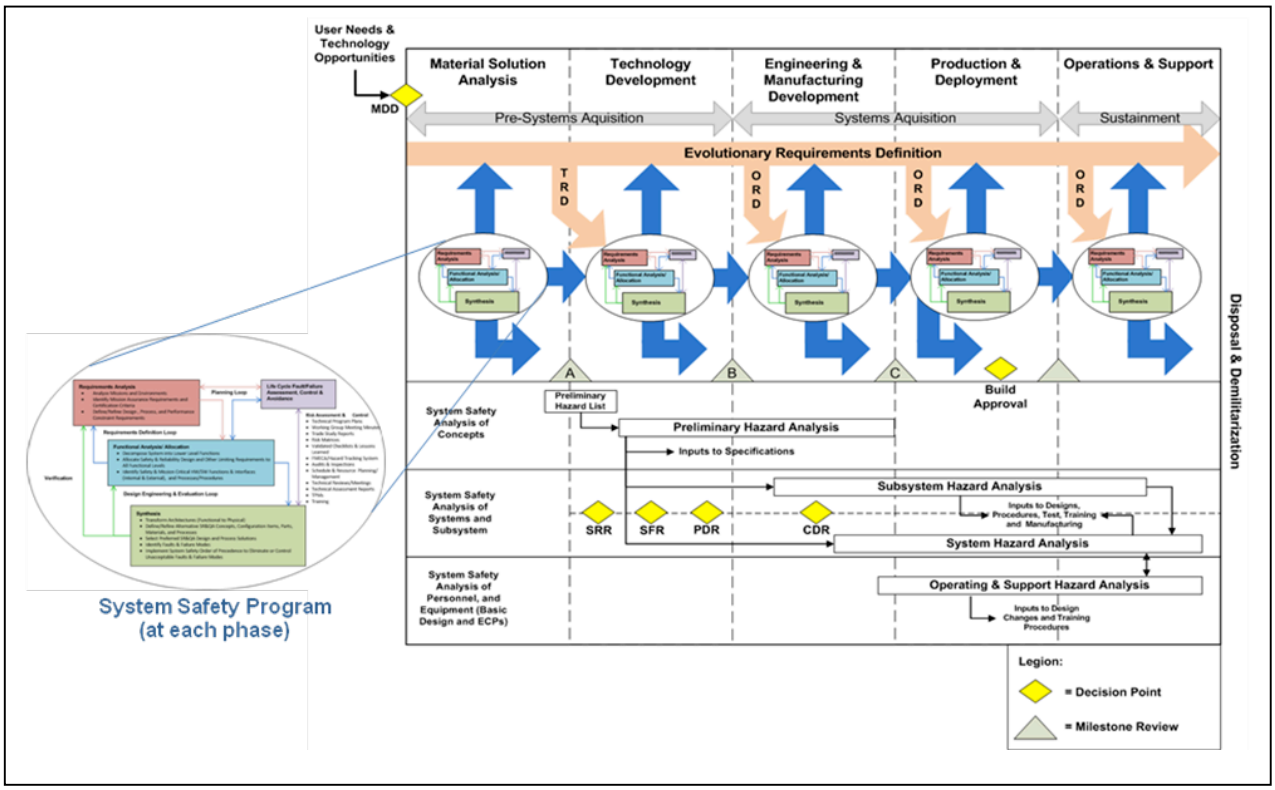

Figure 3: Progressive Implementation of System Safety Program in the Product Life Cycle.

1.3 Applicability

SET's strengths in systems analysis, architecture and design are consistent and coherent. Yet the application of system safety practices in past technology development was hit-and-miss. Based upon sage advice and cogent reasoning since then, *SET* has embarked on a company-wide endeavor to institutionalize a structured capability-based system safety philosophy throughout the company's systems engineering process. Accordingly, *SET* is committed to applying the capability-based system safety program in the development of all of its products.

The "capability-based" aspect of this Standard involves implementing a system safety programs in accordance with predefined processes that are tailored for cost-effective identification, evaluation, and mitigation or control of specific existing and potential deficiencies that pose a threat to system safety or mission success, throughout the product's useful life and post-mission disposal. These deficiencies include damage-threatening hazards, mission-impacting failures modes, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

2. REFERENCES

2.1 Normative References

The following reference documents of the issue in effect on the date on invitation for bid or request for proposal form a part of this Standard to the extent specified:

AIAA S-102.1 Mission Assurance Management

1) AIAA S-102.0.1 (Draft)	Mission Assurance Program General Requirements
2) AIAA S-102.1.1 (Draft)	Mission Assurance Program Planning Requirements
3) AIAA S-102.1.2 (Draft)	Subcontractor and Supplier Mission Assurance Management Requirements
4) AIAA S-102.1.3 (Draft)	Mission Assurance Working Group (MAWG) Requirements
5) AIAA S-102.1.4 (Released)	Failure Reporting, Analysis and Corrective Action System (FRACAS) Requirements
6) AIAA S-102.1.5 (Released)	Failure Review Board (FRB) Requirements
7) AIAA S-102.1.6 (Draft)	Critical Item Risk Management (CIRM) Requirements
8) AIAA S-102.1.7 (Draft)	Project Mission Assurance Database System Requirements
9) AIAA S-102.1.8 (Draft)	Quality Assurance (QA) Requirements
10) AIAA S-102.1.9 (Draft)	Configuration Management (CM) Requirements
11) AIAA S-102.1.10 (Draft)	Environmental Safety Assurance Requirements

AIAA S-102.2 Mission Assurance Engineering and Analysis

12) AIAA S-102.2.1 (Draft)	Functional Diagram Modeling (FDM) Requirements
13) AIAA S-102.2.2 (Released)	System Reliability Modeling Requirements
14) AIAA S-102.2.3 (Draft)	Component Reliability Predictions Requirements
15) AIAA S-102.2.4 (Released)	Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements
16) AIAA S-102.2.5 (Draft)	Sneak Circuit Analysis (SCA) Requirements
17) AIAA S-102.2.6 (Draft)	Design Concern Analysis (DCA) Requirements
18) AIAA S-102.2.7 (Draft)	Finite Element Analysis (FEA) Requirements
19) AIAA S-102.2.8 (Draft)	Worst Case Analysis (WCA) Requirements
20) AIAA S-102.2.9 (Draft)	Human Error Predictions Requirements
21) AIAA S-102.2.10 (Draft)	Environmental Event Survivability Analysis Requirements

22) AIAA S-102.2.11 (Released) Anomaly Detection and Response Analysis Requirements

23) AIAA S-102.2.12 (Draft) Maintainability Predictions Requirements

24) AIAA S-102.2.13 (Draft) Operational Dependability and Availability Modeling Requirements

25) AIAA S-102.2.14 (Draft) Hazard Analysis (HA) Requirements

26) AIAA S-102.2.15 (Draft) Software Component Reliability Predictions Requirements

27) AIAA S-102.2.16 (Draft) Process Failure Mode, Effects, and Criticality Analysis (FMECA) Requirements

28) AIAA S-102.2.17 (Draft) Event Tree Analysis (ETA) Requirements

29) AIAA S-102.2.18 (Draft) Fault Tree Analysis (FTA) Requirements

30) AIAA S-102.2.19 (Draft) Fishbone Analysis Requirements

31) AIAA S-102.2.20 (Draft) Similarity and Allocations Analysis Requirements

32) AIAA S-102-2.21 (Draft) Component Engineering Requirements

33) AIAA S-102.2.22 (Draft) Stress and Damage Simulation Analysis Requirements

AIAA S-102.3 Mission Assurance Testing

34) AIAA S-102.3.1 (Draft) Environmental Stress Screening (ESS) Requirements

35) AIAA S-102.3.2 (Draft) Reliability Development / Growth Testing (RD/GT) Requirements

36) AIAA S-102.3.3 (Draft) Reliability, Maintainability, and Availability Demonstration Testing Requirements

37) AIAA S-102.3.4 (Draft) Reliability Life Testing Requirements

38) AIAA S-102.3.5 (Draft) Design of Experiments Requirements

39) AIAA S-102.3.6 (Draft) Ongoing Reliability Testing (ORT) Requirements

40) AIAA S-102.3.7 (Draft) Product Safety Testing Requirements

Corporate References

41) Reliability Design Rules (Draft)

42) Joint Services Software Safety Design Rules (Released)

2.2 Relationship to Other Corporate Standards

This Standard falls under the *SET* Corporate Standard for the Mission Assurance Program, and aligns with the *SET* Corporate Standards for the Reliability, Maintainability, Availability & Dependability (RMAD) Program, and the Quality Assurance (QA) Program. This Standard

defines the set of activities that aid identification, evaluation, and mitigation or control of existing and potential hazards in all life cycle phases of the product.

3. Terminology

3.1 Terms and Definitions

anomaly
apparent problem or failure affecting a configured product, process, or support equipment/facilities that is detected during product verification or operation
NOTE: Anomalies are distinguished from discrepancies, product defects which do not violate project requirements which may or may not be documented in the FRACAS.

acquisition authority
an organization (Government, contractor, or subcontractor) that levies requirements on another organization through a contract or other document

approximation[1]
a value that is nearly but not exactly correct or accurate

audit
an independent examination of accounts and records to assess or verify compliance with specifications, standards, contractual agreements, or other criteria (Ref. IEEE STD 1624-2008)

baseline process
the minimum set of functions that constitute a specific type of process

baseline program
the minimum set of functions that constitute a specific type of program

capability
one or more processes or activities that describe how SR&QA programs are used, treated, or developed within an organization (Ref. IEEE STD 1624-2008)

capability-based system safety program
the set of processes that assesses and controls product deficiency risk at one or more predefined capability levels

capability level
measure of the ability of a system safety process, as specified by a set of activities, to address the pertinent system safety needs of a systems engineering process

[1] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

capability level growth
a measurable improvement (e.g., an increase in resources, scope of effort, or maturity of input data) in the ability of a system safety process to support the system safety needs of a systems engineering process

chaos
the random occurrence of unpredictable and unrelated events

control
a method used to reduce the consequences, likelihood, or effects of a hazard or failure mode
NOTE: Controls include special design features, procedures, inspections, or tests

credible failure mode or hazard
a failure mode or hazard with a probability of occurrence greater than $1.0E^{-6}$, 0.000001, or one in a million

engineering judgment
a properly trained engineer's technical opinion that is based on an evaluation of specific data and personal experience
NOTE: Engineering judgments are a reality that cannot not be avoided when insufficient time, data, or funding are available to perform a detailed quantitative analysis.

environmental safety assurance
to give appropriate consideration to potential environmental impacts prior to beginning any action that may significantly affect the environment

estimation
a tentative evaluation or rough order magnitude calculation

failure
termination of the ability of a unit to perform its required function
NOTE: A fault may cause a failure.

failure mode
consequence of the mechanism through which a failure occurs, or the manner by which a failure is observed

fault[2]
[1] [Software reliability] a manifestation of an error in software; [2] [Hardware reliability] any undesired state of a component or system; [3] [Components] a defect or flaw in a hardware or software component; [4] [Human reliability] procedure (operational or maintenance) or process (manufacture or design) that is improperly followed;

[2] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

NOTES: [1] An accident may cause a fault; [2] A fault may cause a failure; [3] A fault does not necessarily require failure.

hazard
a condition that is prerequisite to a mishap and a contributor to the effects of the mishap
NOTE: A single point failure mode (SPFM) item is a hazard with respect to its potential to lead directly to loss of a safety-critical or mission-critical system function.

maturity level
measure of the degree of accuracy of a data product, as developed using a specified set of input data, in relation to what is considered the best achievable results

method
a formal, well-documented approach for accomplishing a task, activity, or process step governed by decision rules to provide a description of the form or representation of the outputs (C/SE) 1220-1994s

mishap
an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

mission
the purpose and functions of the space system (sensors, transponders, boosters, experiments, etc.) throughout its expected operational lifetime, and controlled reentry or disposal orbit time period. A space system may have multiple missions (e.g., primary mission, ancillary mission, and safety mission)

mission assurance
the program-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to system safety or mission success, throughout the product's useful life and post-mission disposal
NOTE:Deficiencies include damaging-threatening hazards, mission-impacting failures, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

mission capability
This term encompasses the purpose and functions of the space system (sensors, transponders, etc.) throughout its intended system mean mission duration (the expected life of the space vehicle). (Ref. AFMAN 91-222 SUPL1)

mitigation
(1) a method that eliminates or reduces the consequences, likelihood, or effects of a hazard or failure mode; (2) a hazard control

modeling
act of producing a representation or simulation of one or more items

non-credible failure mode or hazard
a failure mode or hazard with a probability of occurrence equal to or less than 1.0E-6, 0.000001, or one in a million
NOTE: In System Safety Engineering, the qualitative probability values of an improbable hazard and a non-credible hazard are equivalent.

plan
a method for achieving an end

practice
one or more activities that use specified inputs to develop specified work products for achieving specified objectives (Ref. IEEE Standard 1624-2008)

process-based lesson learned
important information created, documented, and retrieved according to a process or procedure descriptor

product-based lesson learned
important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor

program
[1] the managed collection of an organization's practices that is structured to ensure that the customers' requirements and product needs are satisfied (Ref. IEEE Standard 1624-2008); [2] a defined set of managed processes conducing to an end under a single plan
NOTE: A program does not have to consist of related, managed process. Compare with definition of *"system"*.

process
a sequence of tasks, actions, or activities, including the transition criteria for progressing from one to the next, that bring about a result (Ref. IEEE Standard 1624-2008)
NOTE: A process can be unmanaged or managed. An unmanaged or "free" process does not have its inputs or outputs controlled. The rain and melted snow that replenishes a lake is an example of an unmanaged process. A managed or "controlled" process has its inputs and outputs controlled. An electrical power station is an example of a managed process.

quality
a measure of a part's ability to meet the workmanship criteria of the manufacturer
NOTE: Quality levels for parts used by some of the handbook methods are different from quality of the parts. Quality levels are assigned based on the part source and level of screening the part goes through. The concept of quality level comes from the belief that screening improves part quality.

reliability
probability that an item will perform its intended function for a specified interval under stated conditions

residual risk
risk associated with significant failure modes or hazards for which there are no known control measures, incomplete control measures, or no plans to control the failure mode or hazard

root cause(s)
most fundamental reason(s) an event might or has occurred

root cause analysis
a process for identifying the fundamental cause of an event or failure

safety
freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

safety critical
a term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component

specialty engineering
a subgroup of the engineering processes that make up the Mission Assurance Process
Note: Traditionally, this subgroup includes Reliability, Maintainability, PMP, Survivability, and Supportability.

system
[1] a defined set of related processes
[2] elements of a composite entity, at any level of complexity of personnel, procedures, materials, tools, equipment, facilities, and software, that are used together in an intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement
NOTE: A system that consists of one or more unmanaged processes is susceptible to becoming "unbalanced" and changing over time (e.g., an ecological system). For a system to maintain stability it must be "balanced" and consist only of managed processes.

system safety
the application of engineering management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle (Ref. MIL-STD-882C)

systems engineering
An interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and life-cycle balance set of system product and process solutions that satisfy customer needs. (Ref. MIL-STD-499B Draft)

tailoring
process by which the individual requirements (tasks, sections, paragraphs, words, phrases, or sentences) of a standard are evaluated to determine the extent to which each requirement is most suited for a specific system acquisition and the modification of these requirements, where necessary, to ensure that each tailored document invokes only the minimum needs of the customer

timely
performance of a task, subtask, or effort when planning and execution results in the output being provided with sufficient time for management, if need be, to identify and implement cost-effective action
EXAMPLE: An action that avoids or minimizes schedule delays and cost increases.

validation
the act of determining that a product or process, as constituted, will fulfill its desired purpose

verification
the process of assuring that a product or process, as constituted, complies with the requirements specified for it

3.2 Acronyms

A_O	Availability Analysis
CA	Criticality Analysis
CIRM	Critical Item Risk Management
CN	Criticality Number
DCA	Design Concern Analysis
D_O	Dependability Analysis
ECP	Engineering Change Proposal
EOLP	End of Life Plan
ESS	Environmental Stress Screening
ETA	Event Tree Analysis
ETC	Estimate to Complete
FDM	Functional Diagram Modeling
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and corrective Action
FRB	Failure Review Board
FTA	Fault Tree Analysis
HA	Hazard Analysis
HW	Hardware
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
LLAA	Lessons Learned Approval Authority
LOE	Level of Effort
MAP	Mission Assurance Program
	Mission Assurance Process

MAPP	Mission Assurance Program Plan
	Mission Assurance Program Planning
MCLP	Multiple Capability Level Process
O&SHA	Operating and Support Hazard Analysis
PMP	Parts, Materials & Processes
PoF	Physics of Failure
QA	Quality Assurance
R&M	Reliability and Maintainability
RD/GT	Reliability Development/Growth Testing
RMAD	Reliability, Maintainability, and Availability Demonstration
	Reliability, Maintainability, Availability and Dependability
SCA	Sneak Circuit Analysis
SCLP	Single Capability Level Process
SEC	Standards Executive Council
SEMP	Systems Engineering Management Plan
SPFM	Single Point Failure Mode
SR&QA	Safety, Reliability & Quality Assurance
SSP	System Safety Program
SW	Software
SSWG	System Safety Working Group
TAAF	Test, Analyze and Fix
TPM	Technical Performance Metrics
V&V	Verification & Validation

4. General Requirements

4.1 System Safety Program Task Selection

This Standard provides the foundation for tailoring *SET's* system safety programs to be commensurate with the hazard severity and life cycle phase of the product it is applied to. Accordingly, *SET's* System Safety Programs will be implemented in accordance with the groups of tasks shown in the columns in Table 2. These groups of tasks represent a capability-based approach to system safety that is cost-effective and repeatable, and as such, will be extensible into pristine technical territory in the future.

Table 2: System Safety Program Task Selection Based on System Dollar Value & Worst Case Hazard Severity.

Less Than $50K System Value and Hazard Severity Level IV	$50K to Less Than $500K System Value and Hazard Severity Level IV	$500K to Less Than $2M System Value or Less Than $500K and Hazard Severity Level III	$2M or Higher System Value or Hazard Severity Level I or II
TASK 101 - System Safety Program Authorization, Safety Design Requirements Definition & Risk Mgmt	TASK 101 - System Safety Program Authorization, Safety Design Requirements Definition & Risk Mgmt	TASK 101 - System Safety Program Authorization, Safety Design Requirements Definition & Risk Mgmt	TASK 101 - System Safety Program Authorization, Safety Design Requirements Definition & Risk Mgmt
TASK 102 – System Safety Program Planning & Coordination	TASK 102 - System Safety Program Planning & Coordination	TASK 102 - System Safety Program Planning & Coordination	TASK 102 - System Safety Program Planning & Coordination
TASK 103 - Integration/Mgmt of Contractors	TASK 103 - Integration/Mgmt of Contractors	TASK 103 - Integration/Mgmt of Contractors	TASK 103 - Integration/Mgmt of Contractors
TASK 201 - Preliminary Hazard List (2)	TASK 105 - SSG/SSWG	TASK 105 - SSG/SSWG	TASK 104 - Reviews/Audits
TASK 202 - Preliminary Hazard Analysis	TASK 106 - Hazard Tracking	TASK 106 - Hazard Tracking	TASK 105 - SSG/SSWG
TASK 205 - System Hazard Analysis	TASK 201 - Preliminary Hazard List (2)	TASK 201 - Preliminary Hazard List (2)	TASK 106 - Hazard Tracking
TASK 401 - Safety Requirements Verification	TASK 202 - PHA (2)	TASK 202 - PHA (2)	TASK 107 - Safety Progress Reports
	TASK 203 - Safety Requirements/Criteria Analysis (2)	TASK 203 - Safety Requirements/Criteria Analysis (2)	TASK 201 - Preliminary Hazard List (2)
	TASK 205 - System Hazard Analysis	TASK 204 – Subsystem Hazard Analysis	TASK 202 - PHA (2)
	TASK 302 - Test and Evaluation Safety (2)	TASK 205 - System Hazard Analysis	TASK 203 - Safety Requirements/Criteria Analysis (2)
	TASK 303 - Safety ECPs	TASK 301 - Safety Assessment	TASK 204 – Subsystem Hazard Analysis
	TASK 401 - Safety Requirements Verification	TASK 302 - Test and Evaluation Safety (2)	TASK 205 - System Hazard Analysis
		TASK 303 - Safety ECPs	TASK 206 – Operating & Support Hazard Analysis
		TASK 401 - Safety Requirements Verification	TASK 207 – Health Hazard Assessment (3)
		TASK 402 - Safety Compliance Assessment	TASK 301 - Safety Assessment
			TASK 302 - Test and Evaluation Safety (2)
			TASK 303 - Safety ECPs
			TASK 401 - Safety Requirements Verification
			TASK 402 - Safety Compliance Assessment
			TASK 403 - Explosive Hazard Class
			TASK 404 - Explosive Ordnance Disposal Source Data

NOTES: (1) Each task is to be tailored based the implementation details stated in the SOW
(2) These tasks may applicable to only one phase of the program
(3) To avoid duplication in effort, Health Hazard Assessment (HHA) should leverage off O&SHA data and Materials and Processes (M&P) data

4.2 System Safety Data Item Descriptions

System safety data item descriptions (DIDs) describe the data content and format of contractor generated documents. The relationship between MIL-STD-882C tasks and the DIDs that support them is summarized in Table 3. A description of the most common system safety DIDs is provided below:

4.2.1 DI-SAFT-80100A System Safety Program Plan (SSPP).

This plan details the tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate or control hazards throughout the system life cycle. The purpose of this plan is to provide a basis of understanding between the contractor and the managing activity to ensure that adequate consideration is given to safety during all life cycle phases of the program and to establish a formal, disciplined program to achieve the system safety objectives.

4.2.2 DI-SAFT-81300 Mishap Risk Assessment Report (MRAR).

This Data Item report describes format and content preparation instructions for data resulting from the work tasks described in MIL-STD-882C Tasks 201- Preliminary Hazard List; 202 – Preliminary Hazard Analysis; 203 - Safety Requirements/ Criteria Analysis; 204 – Subsystem Hazard Analysis; 205 - System Hazard Analysis; 206 - Operating and Support Hazard Analysis; 207 – Health Hazard Analysis; 301 - Safety Assessment; 302 – Test and Evaluation Safety; 303 – Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Request for Waiver/ Deviation; 401 – Safety Verification; 402 – Safety Compliance Assessment; 403 – Explosive Hazard Classification and Characteristics Data. The data resulting from these tasks and compiled into the MRAR are applicable to the system design, test, processing and operations within a contract.

4.2.3 DI-SAFT-80102A Safety Assessment Report (SAR).

This Data Item report is a comprehensive evaluation of the safety risks being assume prior to test or operation of the system or at contract completion. It identifies all safety features of the system, design, and procedural hazards that may be present in the system being acquired, and specific procedural controls and precautions that should be followed.

4.2.4 DI-SAFT-80101A System Safety Hazard Analysis Report (SSHAR).

This Data Item report documents hazard analyses that are used to systematically identify and evaluate hazards both real and potential, for their elimination or control. It should also be used to define the required format of the Hazard Log.

4.2.5 DI-SAFT-80103A Engineering Change Proposal System Safety Report.

This Data Item report is used to summarize results of analyses, tests and tradeoff studies conducted on proposed engineering design changes throughout the system life cycle.

4.2.6 DI-SAFT-80104A Waiver or deviation System Safety Report.

This Data Item report summarizes the results of analysis, test, and tradeoff studies as they relate to a request for waiver/ deviation. It will identify the risk assessment, mishap potential, and justification associated with results of each waiver or deviation request received throughout the system life cycle.

4.2.7 DI-SAFT-80105A System Safety Program Progress Report.

This SSPPR Data Item can be used to cover periodic reviews of safety activities and to monitor progress of contractor system safety efforts.

4.2.8 DI-SAFT-80106A Health Hazard Assessment Report.

These HHAR Data Items are used to systematically identify and evaluate health hazards, evaluate proposed hazardous materials, and propose measures to eliminate or control these hazards through engineering design changes or protective measures to reduce the risk to an acceptable level.

4.2.9 DI-SAFT-80931 Explosive Ordnance Disposal Data.

This Data Item is used by the Naval Explosive Ordnance Disposal Technology Center (NAVEODTECHCEN) to develop, test, validate and publish joint service non-nuclear explosive ordnance disposal (EOD) 60 series technical orders. EOD technicians will use this data in support of testing, development and operational evaluation of new or modified weapon systems, ordnance items and aerospace systems.

4.2.10 DI-SAFT-81299 Explosive Hazard Classification Data.

The purpose of this Data Item is to obtain the necessary information for assigning hazard classification, such as hazard class/ division, storage compatibility group, and Department of Transportation (DOT) marking. These classifications establish the procedures for the storage and transportation of the item for all user elements.

Table 3: MIL-STD-882C Tasks and DIDs Matrix

Task Description	*DID No.*	*DID Description*
101 - System Safety Program	DI-SAFT-80100A	System Safety Program Plan
102 - System Safety Program Plan	DI-SAFT-80100A	System Safety Program Plan
103 - Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms	Not Applicable	Not Applicable
104 - System Safety Program Reviews/ Audits	Not Applicable	Not Applicable
105 -System Safety Group/System Safety Working Group Support	Not Applicable	Not Applicable
106 - Hazard Tracking and Risk Resolution	[1] DI-SAFT-80101A [2] DI-SAFT-80105A	[1] System Safety Hazard Analysis Report (Definition of Hazard Log Format) [2] System Safety Program Progress Report
107 - System Safety Progress Summary	DI-SAFT-80105A	System Safety Program Progress Report
201 - Preliminary Hazard List	DI-SAFT-80101A	System Safety Hazard Analysis Report
202 - Preliminary Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
203 - Safety Requirements/Criteria Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
204 - Subsystem Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
205 - System Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
206 - Operating and Support Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
207 - Health Hazard Assessment	DI-SAFT-80106A	Health Hazard Assessment Report
301 - Safety Assessment	DI-SAFT-80102A	Safety Assessment Report
302 - Test and Evaluation Safety		
303 - Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/Waiver	DI-SAFT-80103A	Engineering Change Proposal System Safety Report
	DI-SAFT-80104A	Waiver of Deviation System Safety Report
401 - Safety Verification	DI-SAFT-80102A	Safety Assessment Report
402 - Safety Compliance Assessment	DI-SAFT-80102A	Safety Assessment Report
403 - Explosive Hazard Classification and Characteristics Data	DI-SAFT-81299	Explosive Hazard Classification Data
404 - Explosive Ordnance Disposal Data	DI-SAFT-80931	Explosive Ordinance Disposal Data
Multiple Tasks	DI-SAFT-81300	Mishap Risk Assessment Report

5. DETAILED REQUIREMENTS

The detailed requirements that drive *SET's* system safety programs are found in MIL-STD-882C, except for the following tasks which take precedence.

5.1 Authorization

For all *SET* products regardless of hazard severity level, The System Safety Program will be authorized in accordance with this Standard, and managed independent of the project's management chain, with responsibility and authority to:

- Ensure all applicable environmental, safety, and occupational health (ESOH) requirements are met.
- Evaluate potential ESOH hazards in all applicable life cycle phases of the product.
- Ensure manufacturing, assembly, test, maintenance, storage, transportation, operating, and disposal safety procedures are implemented.

SET will implement a system safety program in all product development projects, either by contractual requirement or by *SET* command media standard practice. If fewer tasks are selected than shown in Figure 1 for the applicable product severity level, then the Lead System Safety Engineer (SSE) is required to provide documentation that verifies no significant hazards will escape identification during the life cycle.

5.1.1 Assignment of Key Personnel

The key system safety engineering personnel are required to meet certain minimum qualifications. Key system safety engineering personnel are usually limited to the persons who have supervisory responsibility/technical approval authority for the system safety work. *SET* personnel assigned to system safety responsibilities will be verified to have the appropriate qualifications (See Table 4) prior to performing system safety related duties. Theses qualifications include the appropriate education, training, and demonstrated ability (through means such as certification and experience) to ensure one can satisfactorily fulfill his/her managerial role and responsibilities. The Lead System Safety Engineer (SSE) will be trained how to select the appropriate system safety activities and tools commensurate with the product hazard severity and life cycle phase.

5.1.2 Lead SSE Responsibilities

The Lead SSE responsibilities include ensuring that sufficient resources are provided to properly assess product and process life cycle hazards. *SET* will acquire validated tools for its system safety programs, on the recommendation of the Lead SSE. The acquired tools will be capable of aiding different disciplines across a project to identify and eliminate or control unacceptable hazards in a timely manner. These tools will facilitate achieving the following objectives:

1. Improve the comprehensiveness, accuracy, timeliness, repeatability, and cost-effectiveness of hazard analyses.
2. Automate the exchange of system safety data to the greatest extent practical.
3. Eliminate the need for the Lead SSE to have permanent system safety staff.
4. Minimize the cost of acquiring and maintaining an integrated system safety toolset.

Table 4: Minimum Qualifications for SET Lead System Safety Engineer

System Dollar Value And Worst Case Hazard Severity[2]	Education	Experience	Training	Certification
$2M or Higher System Value or Hazard Severity Level I or II	BS in Engineering, Physical Science or other[1]	Six years in system safety or related discipline	Cert. System Safety Analysis Course & System Safety Mgmt Course or equivalent[2]	Cert. Safety Profess. (CSP) or Profess. Engr. (Safety)
$500K to Less Than $2M System Value or Less Than $$500K and Hazard Severity Level III	BS in Engineering, Physical Science or other[1]	Four years in system safety or related discipline	Cert. System Safety Analysis Course & System Safety Mgmt Course or equivalent[2]	CSP or Profess. Engr. (Safety)
$50K to Less Than $500K System Value and Hazard Severity Level IV	Bachelor's Degree or other[1] plus training in system safety	Two years in system safety or related discipline	Cert. System Safety Analysis Course & System Safety Mgmt Course or equivalent[2]	Cert. Engr. [3] or Profess. Engr.
Less Than $50K System Value and Hazard Severity Level IV	High School Diploma or other[1] plus training in system safety	Four years in system safety	Cert. System Safety Analysis Course & System Safety Mgmt Course or equivalent[2]	Cert. Technician

(1) The customer may specify other degrees or certifications in the SOW.
(2) NASA provides equivalent safety courses.
(3) Applicability of certified engineers (CQE, CRE, etc.) by professional organizations such as the American Society for Quality (ASQ) will be submitted to the *SET* President for consideration.

5.1.3 Continuous Process Improve

SET has adopted the AIAA Standard S-102.0.1 requirement for Capability Level 5 system safety programs to interface with outside industry organizations and working groups whose charter/goal is to optimize the effectiveness of industry acknowledged mission assurance methods. The types of information to be exchanged with outside industry organizations include non-proprietary lessons learned, hazard reports, component reliability models, and open source computerized tool models.

5.2 Requirement Definition

System safety will identify all systems engineering requirements that oppose a system safety requirement, and coordinate the adjudication of the conflict in accordance with the following requirement order of precedence:

1. Safety critical
2. Mission critical
3. Reliability critical
4. Maintenance critical
5. Monitoring critical

5.2.1 Identify System Safety Requirements That Are Already Met

System safety will identify all system safety requirements that are already satisfied by an existing analysis, inspection, test report, or data product that was developed for a similar project, product, or process. Each satisfied requirement will be identified in the system safety program plan, along with a detailed description of the legacy system, the verification method, and the observed results.

5.3 Planning

The selection of the measureable and level-of-effort (LOE) system safety program tasks are based on: (1) comprehensive coverage of the system safety requirements and self-imposed objectives, (2) optimized balance among system safety costs, schedules, and hazard risk factors, and (3) the applicable system life cycle phases. . Figure 4 is a notional depiction of the trade off that can be made between safety design level of effort versus cost-incurring system characteristics, e.g., prorated loss of system value due to damage-causing mishap.

5.3.1 Plan the Use of Industry Acknowledged Methods

The SSPP will call for the use of industry acknowledged methods to perform all system safety engineering tasks. All of the system safety requirements and their sources will be identified in the Requirements vs. Tasks Matrix in the SSPP. The SSPP also will include a Requirement vs. Responsible Discipline Matrix that identifies all system safety related tasks performed by other disciplines. Each discipline is supposed to have a similar matrix in their respective Plan. Each of these Plans is supposed to identify the tasks that will be performed to achieve the system safety requirements. The Lead System Safety Engineer ensures that these Plans call out the use of industry acknowledged methods to perform the system safety engineering tasks. The SSPP and the other Plans also should include references to public domain documents that describe the basis for industry acknowledgement of the systems engineering methods.

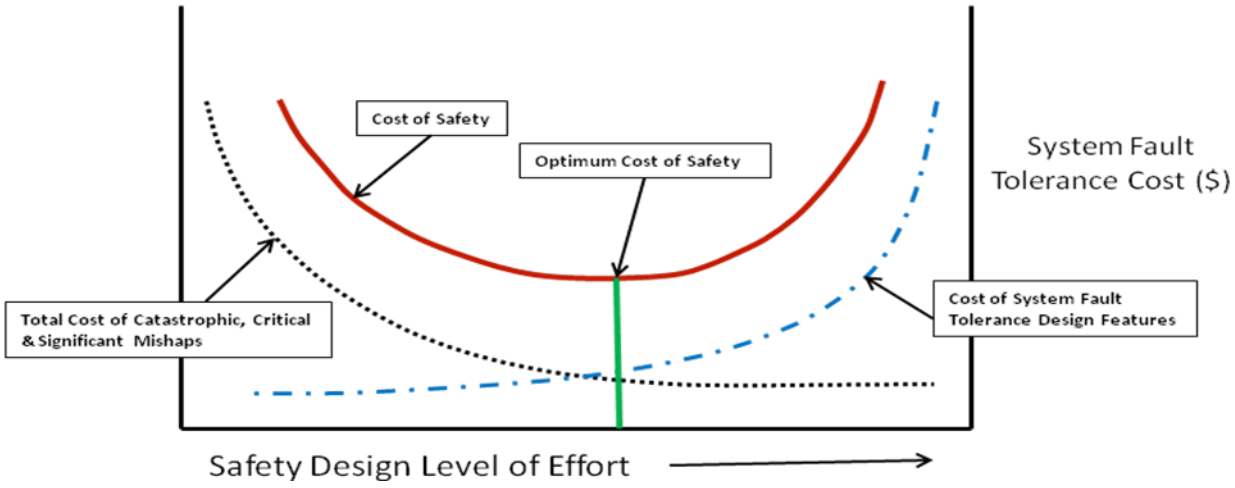

Figure 4: Safety Design Level of Effort Versus Total Mishap Cost

5.4 Coordination

Each systems engineering discipline that has systems safety responsibilities will be identified in the SSPP. The Lead System Safety Engineer (SSE) will develop a set of applicable Defect Avoidance Checklists and distribute them to all system safety stake-holders to enhance their mishap prevention activities. The Lead SSE will also participate in project design reviews, technical interchange meetings, management status reviews, working group meetings, and other meetings that may be germane to system safety, but which are convened by other disciplines, e.g., RMAD and Quality Assurance.

5.5 Engineering and Evaluation

The following product characteristics will be considered unacceptable with regard to safety design risk. Positive action and implementation verification is required to reduce that risk to an acceptable level as negotiated by *SET* and the customer.

a. Single component failure, common mode failure, human error, or design features which could cause a mishap of catastrophic or critical severity.

b. Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of catastrophic or critical severity.

c. Generation of hazardous ionizing/non-ionizing radiation or energy when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

d. Packaging or handling procedures and characteristics which could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.

e. Hazard level categories that are specified as unacceptable in the contract.

f. Human factors capabilities or component designs that fail to address human physical, anthropometrics, physiological, and perceptual-cognitive limitations. For example, a design that is conducive to error, such as, controls that are difficult to read, are confusing, or create excessive cognitive demands on the users.

5.5.1 Identify Hazards

SET will apply industry acknowledged engineering and evaluation principles and techniques to identify eliminate, or control unacceptable hazards, e.g., safety-critical single-fault-tolerant design conditions, and to verify that the hazard risk mitigation/disposition methods are successfully implemented.

5.5.2 Qualitative Risk Likelihood Assessments

Quantitative risk likelihood values are preferred. However, in the absence of a quantitative probability of occurrence analysis, the selection of a qualitative probability value that is based solely on an engineering judgment or guess may be necessary. For all cases where engineering judgment is used in high or serious residual risk acceptance decisions, the source(s) of the engineering judgment will be identified and verified to have several years of experience in performing detailed reliability predictions on systems, equipment, or processes similar to the one being assessed. Qualitative probability values will follow the same ground rules as qualitative severity categories. They will be defined in sufficient detail to allow different people to independently arrive at the same conclusion when reviewing the same input data. The system safety definitions in Figure 5, for probability of occurrence and severity categories, will be used in all system safety analyses, evaluations, and tests.

5.5.3 Use Industry Acknowledged Engineering Methods

System safety will use industry acknowledged methods to perform all system safety engineering tasks. The engineering reports generated by system safety should include references to public domain documents that describe the basis for industry acknowledgement of the systems engineering methods used. System Safety will also ensure that the analytical assumptions are identified and assessed with regard to their maturity for all system safety engineering related tasks performed by other disciplines.

Table 5: Hazard Severity and Probability of Occurrence Category Definitions

Value/ Level	Occurrence		Severity		
	Reliability Definitions	System Safety Definitions	Reliability Definitions		System Safety Definitions
5	Very High (1 in 10 or greater)	(A) FREQUENT (X > 10^-1)	1 - Complete loss of mission: complete loss of primary mission capability.		I - 1 - CATASTROPHIC Death, system loss, or severe environmental damage.
4	High (less than 1 in 10 but greater than 1 in 20)	(B) PROBABLE (10^-1 > X > 10^-2)	2 - Major loss or degradation of the primary mission: capability to complete some mission objectives (or all at a degraded level) with immediate loss of a critical science instrument; or loss of a major amount of critical science data; or major reduction in life of the primary mission; or loss of spacecraft function resulting in loss of opportunity for obtaining critical science data.		II - 2 - CRITICAL Severe injury, severe occupational illness, major system or environmental damage.
3	Moderate (less than 1 in 20 but greater than 1 in 100)	(C) OCCASIONAL (10^-2 > X > 10^-3)	3 - Minor loss or degradation of the primary mission: minor loss of spacecraft or instrument function leading to loss of a minor amount of critical science data; or a significant reduction in life of the primary mission; or loss or major degradation of an ancillary mission.	1R - Loss or degradation of a redundant subsystem or science instrument producing level 5 severity, if remaining redundancy is lost.	III - 3 - MARGINAL / SIGNIFICANT Minor injury, minor occupational illness, or minor system or environmental damage.
2	Low (less than 1 in 100 but greater than 1 in 500)	(D) REMOTE (10^-3 > X > 10^-6)	4 - Potential for less than minor loss or degradation of spacecraft or performance: no immediate impact on spacecraft or primary mission, but potential exists for future loss, at severity levels 3 to 5, due to induced failure or resulting from the conjunction of this anomaly with a future event; or potential for cumulative major loss of a mission-critical function over a long period of time; or spacecraft or primary mission loss or significant degradation, at severity level 4, would occur if adequate redundancy, alternatives, or compensating measures are not implemented; or minor degradation of an ancillary mission.	2R - Loss or degradation of a redundant subsystem or science instrument, producing a level 4 severity, if remaining redundancy is lost.	IV - 4 - NEGLIGIBLE Less than minor injury, occupational illness, or less than minor system or environmental damage.
1	Very Low (less than 1 in 500)	(E) IMPROBABLE / NON-CREDIBLE (10^-6 > X)	5 - Insignificant or no impact on spacecraft life or performance: barely noticeable or no performance degradation, and fault does not lead to loss or degradation of instrument data; or loss of significant amount ofancillary mission data; or significant peril to spacecraft or primary mission, at severity level 3, would occur if adequate redundancy, alternatives, or compensating measures are not implemented; or less than minor degradation of an ancillary mission.	3R - Loss or degradation of a redundant subsystem or science instrument, producing a level 3 severity, if remaining redundancy is lost.	V - 5 - NONE / INSIGNIFICANT Failure modes that would have no loss or effects to mission objectives or the environment, or no injuries.

5.5.4 Perform Structured Evaluations

If a Capability Level 5 or higher system safety program is required, *SET* will develop and apply a structured review process (e.g., a formal peer review working group) to aid thorough evaluation of the system safety program output artifacts in all product life cycle phases. The review process will include personnel who are cognizant of events that led to hazards in systems similar to the one being developed. Product-based and process-based lessons learned that are relevant to the system being developed will be gathered across the enterprise and used to develop review checklists that support timely implementation of the structured review process and updating of

the system safety program. The review checklists will reflect the technical knowledge, insights, design rules, application data, and other clues that helped uncover hazards in the past. The types of systems engineering artifacts that should be independently reviewed shall include, but are not limited to, those listed in Table 6.

Table 6: Sample Systems Engineering Artifacts.

NAME OF DOCUMENT	ARTIFACT CATEGORY
Anomaly Detection and Resolution (ADR) Design Description	Engineering & Evaluation
Approved Parts & Materials List (APML)	Program Coordination
Command Media (Contractor's Internal Practices)	Program Authorization
Critical Item List (CIL)	Engineering & Evaluation
Engineering Memorandum	Engineering & Evaluation
Environmental Analysis Data Report	Engineering & Evaluation
Disposal Plan	Planning
Failure Mode, Effects and Criticality Analysis (FMECA)	Engineering & Evaluation
Fault Tree Analysis (FTA)	Engineering & Evaluation
Failure Report	Engineering & Evaluation
FRACAS Plan	Planning
Hazard Report (HR)	Engineering & Evaluation
Hazard Risk Assessment Matrix (HRAM)	Risk Tracking
Hazardous Material Management Program (HMMP) Report	Planning
Indentured Parts List	Program Coordination
Integrated Master Plan (IMP)	Planning
Integrated Master Schedule (IMS) (Contractor's SR&QA Programs)	Planning
Lessons Learned Report	Program Coordination
Mishap Investigation Plan (MIP)	Planning
Mishap Risk Assessment Report (MRAR)	Engineering & Evaluation
Missile System Pre-launch Safety Packages (MSPSP)	Engineering & Evaluation
NEPA Facilitation Report	Engineering & Evaluation
On-orbit Operations Handbook (OOH)	Program Coordination
Operational Dependability Analysis	Engineering & Evaluation
Part Stress Derating Analysis	Engineering & Evaluation

NAME OF DOCUMENT	ARTIFACT CATEGORY
Parts, Materials, and Processes (PMP) Program Plan	Planning
Preliminary Hazard Analysis (PHA)	Engineering & Evaluation
Preliminary Hazard List (PHL)	Engineering & Evaluation
Quality Assurance (QA) Program Plan	Planning
Reliability Life Test Plan	Planning
Request for Proposal	Requirements
Risk Management/Mitigation Process Plan	Planning
RMAD Analysis/Assessment Report	Engineering & Evaluation
RMAD Plan	Planning
Safety Assessment Report (SAR)	Engineering & Evaluation
Space Vehicle Survivability Analysis	Engineering & Evaluation
Statement of Work (SOW)	Requirements
Subsystem Hazard Analysis (SSHA)	Engineering & Evaluation
System Hazard Analysis (SHA)	Engineering & Evaluation
System Reliability Assessment Report	Engineering & Evaluation
SR&QA Program Plans	Planning
SR&QA Status Reports	Program Coordination
SR&QA Working Group Meeting Agenda/Briefing Charts/Minutes/Action Items	Program Coordination
System Specification	Program Coordination
Systems Engineering Management Plan (SEMP)	Planning
System Safety Program Plan	Planning
System Safety Program Status Report	Engineering & Evaluation
Test Plan	Planning
Test Report	Verification
Waivers	Risk Tracking

The applicable system safety program artifacts shall be used to evaluate the system safety program, in accordance with the criteria shown in Table 7:

Table 7: System Safety Program Evaluation Criteria.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
Program Authorization	1	The contractor has an industry acknowledged basis for authorizing its System Safety Program.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C **OUTPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) System Safety Program Plan and System Safety Working Group (SSWG) charter	(a) Output document references specific excerpts from AIAA Standard S-102.0.1 or MIL-STD-882C as basis for authorization of the System Safety Program. (b) System Safety Program authorization includes the contractor's recognition of specific organizations, managers, staff, working groups, procedures, and responsibilities.
	1	The contractor has an industry acknowledged basis for establishing the minimum qualifications of the Lead System Safety Engineer.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C **OUTPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) System Safety Program Plan and System Safety Working Group (SSWG) charter	(a) Output document references specific excerpts from AIAA Standard S-102.0.1 or MIL-STD-882C as basis for establishing the Lead System Safety Engineer's minimum qualifications. (b) Lead System Safety Engineer's qualifications include minimum college degrees and minimum years of directly related experience.
	2	The contractor has an industry acknowledged basis for establishing empowering policies to facilitate effective execution of the System Safety Program.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C **OUTPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) System Safety Program Plan and System Safety Working Group (SSWG) charter	(a) Output document describes specific excerpts from AIAA Standard S-102.0.1 or MIL-STD-882C as basis for empowering the Lead System Safety Engineer with the power to effectively execute the System Safety Program. (b) Lead System Safety Engineer's empowering responsibilities include reporting system safety risks directly to the project director, and coordinating all of the system safety related activities that are performed by other disciplines.
	3	The contractor has an industry acknowledged basis for acquiring resources to facilitate cost-effective execution of the System Safety Program.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C **OUTPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) System Safety Program Plan and System Safety Working Group (SSWG) charter	(a) The output document describes specific excerpts from AIAA Standard S-102.0.1 or MIL-STD-882C as basis for acquiring resources to facilitate cost-effective execution of the System Safety Program. (b) System Safety Program resources include the project-wide parts engineering database, and system safety engineering checklists to be used by all system safety stakeholders in the project.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
	4 & 5	The contractor has an industry acknowledged basis for interfacing with outside industry organizations and working groups whose charter/goal is to optimize the effectiveness of industry acknowledged quality assurance methods.	**INPUT:** (a) AIAA Standard S-102.0.1 **OUTPUT:** (a) Memorandum of Understanding (b) Contractor's Internal System Safety Program Command Media	(a) Output document describes specific excerpts from AIAA Standard S-102.0.1 as basis for interfacing with outside industry organizations and working groups whose charter/goal is to maximize the effectiveness and minimize the risk of industry recognized system safety engineering methods. (b) The types of information to be exchanged with outside industry organizations include non-proprietary lessons learned, hazard reports, component reliability models, and open source computerized tool models.
Requirements Definition	1	All of the applicable environment, safety, and occupational safety (ESOH) requirements (including regulatory and certification requirements) and self-imposed objectives are identified by the Lead System Safety Engineer using System Requirements Analysis methods.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUT:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) System safety requirement verification plan (RVP)	(a) All of the system safety requirements and their sources are identified in the Requirements vs. Tasks Matrix in the SSPP. (b) Each discipline is supposed to have a similar matrix in their respective Plan to identify the tasks that will be performed to achieve their particular system safety requirements. (c) The system safety design requirements are identified in the draft requirement verification plan (RVP).
	1	All implemented safety critical processes are required to be actively controlled.	**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) Systems Engineering Management Plan (e) Integrated Master Plan **OUTPUT:** (a) Work Breakdown Structure (b) Quality Assurance Program Plan (QAPP)	(a) The contractor's WBS establishes active control over all implemented systems engineering processes. (b) All identified safety-critical processes are identified in the Requirements vs. Tasks Matrix in the QAPP.
	1	The applicable system safety requirements (including regulatory and certification requirements) are incorporated in all program documents that impact product safety.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter	(a) All of the system safety requirements and their sources are identified in the Requirements vs. Tasks Matrix in the SSPP. (b) SSPP includes a requirement versus responsible discipline matrix that identifies all of the system safety requirements that other disciplines in Systems Engineering have. Each discipline is supposed to have a similar matrix in their respective Plan. These Plans are supposed to identify the tasks that will be performed to achieve the system safety requirements.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			(b) Individual Systems Engineering Discipline Plans (c) Product specifications	
	1	All of the required deliverables are identified, along with the required reporting format for each one.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans	(a) The customer's Statement of Work (SOW) and the contractor's subcontractor RFP/SOW identifies the required deliverables, along with their required reporting formats. (b) The SOW may call out deliverables identified in AIAA Standard S-102.0.1 or MIL-STD-882C. (c) All of the system safety requirements and their sources are identified in the Requirements vs. Tasks Matrix in the SSPP. (d) SSPP includes a requirement versus responsible discipline matrix that identifies all of the system safety requirements that other disciplines in Systems Engineering have. Each discipline is supposed to have a similar matrix in their respective Plan that identifies the tasks they will perform to achieve their system safety requirements.
	2	All applicable system safety requirements are flowed down to internal stakeholder and subcontractors.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans (c) Subcontractor SOW (d) Subcontractor SSPP	(a) All of the internal system safety stakeholders and subcontractors are identified in the SSPP, along with their flowed down system safety requirements. (b) The subcontractor SOW identifies the flowed down system safety requirements. (c) Each subcontractor's SSPP identifies the tasks to achieve their flowed down system safety requirements.
	3	The use of industry acknowledged system safety engineering methods is required of all systems engineering disciplines that perform system safety engineering/analytical tasks.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans (c) Systems Engineering Discipline Engineering and	(a) Contractor's Internal System Safety Program Command Media requires all systems engineering disciplines to use industry acknowledged analytical methods. (b) The SSPP and Systems Engineering Discipline Plans and Reports should identify their analytical methods and the references to industry acknowledgements.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			Evaluation Reports	
	3	Overlooked, unnecessary, or incorrect system safety requirements are identified by using Decision Analysis, Mission Analysis, and Requirements Hazard Analysis, or equivalent methods.	**INPUTS:** (a) Decision Analysis Report (b) Mission Analysis Report (c) Requirements Hazard Analysis Report **OUTPUT:** (d) Risk Management Database Report	(a) Contractor's Risk Management Database Report identifies overlooked, unnecessary, or incorrect system safety requirements.
	3	Approved waivers are provided for all unmet contract-specified functional performance requirements, and approved exceptions are provided for all unmet contractor-specified configuration requirements.	**INPUTS:** (a) SEMP (b) IMP (c) Systems Engineering Discipline Engineering and Evaluation Reports (d) Requirement Verification Report **OUTPUTS:** (a) Risk Management Database Report (b) Approved Waiver Report	(a) The requirement for an approved waiver to be provided for all unmet contract-specified functional performance requirements should be called out in the SEMP and the IMP. (b) Collectively, the Systems Engineering Discipline Engineering and Evaluation Reports should identify all unmet requirements. (c) Approved Waiver Reports document the contractors rational for not meeting a significant requirement.
	4 & 5	Criteria and frequency for self-inspections, and subcontractor proposal evaluations and audits are established.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C **OUTPUT:** (a) Contractor's Internal System Safety Program Command Media	(a) AIAA Standard S-102.0.1and MIL-STD-882C provides guidance for self-inspections. (b) Contractor's internal System Safety Program Command Media defines the criteria and frequency for self-inspections, subcontractor proposal evaluations, and subcontractor audits.
	4 & 5	The identification of analytical assumptions that are used in system safety engineering/analytical tasks is required of all systems engineering disciplines.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans	(a) Contractor's Internal System Safety Program Command Media requires all systems engineering disciplines to identify their analytical assumptions (b) SSPP and Plans generated by other systems engineering disciplines should include requirement to identify their analytical assumptions.
	4 & 5	System safety defines the standardized formats for exchanging system safety engineering data, including subcontract system safety deliverables.	**INPUT:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C DIDs **OUTPUT:** (a) Contractor's Internal System Safety Program Command Media	(a) AIAA Standard S-102.0.1and MIL-STD-882C DIDs provides guidance for standardized formats used to exchange system safety engineering data,. (b) Contractor's Internal System Safety Program Command Media defines the required formats for exchanging system safety engineering data, including subcontract system safety data deliverables.
Planning (Including Test Plans)	1		**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C	(a) SSPP includes a requirement versus task matrix that identifies all of the tasks that system safety will perform to achieve their system safety

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
		System Safety Program Plan (SSPP).	(c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans	requirements. (b) Each discipline is supposed to have a matrix in their respective Plan that identifies the tasks they will perform to achieve their system safety requirements.
	1	All applicable ESOH requirements (including safety certifications and self-imposed objectives) that must be achieved by other disciplines are identified in the respective Plans of those disciplines and in the SSPP. NOTE: The Plans of other disciplines include the Systems Engineering Management Plan, the Integrate Master Plan, and the Risk Management Plan.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Systems Engineering Management Plan (SEMP) (c) Integrate Master Plan (IMP) (d) Risk Management Plan (e) Quality Improvement Plan (f) System Safety Program Plan (g) RMAD Program Plan (h) End of Life Plan (EOLP)	(a) SSPP includes a requirement versus task matrix that identifies all of the tasks that system safety will perform to achieve their system safety requirements. (b) SSPP also includes a requirement versus responsible discipline matrix that identifies all of the system safety requirements that other disciplines in Systems Engineering are responsible for achieving. (c) Each discipline is supposed to have a similar matrix in their respective Plan to identify their applicable system safety requirements.
	2	The selection of the measureable and level-of-effort (LOE) system safety tasks are based on: (1) comprehensive coverage of the system safety requirements and self-imposed objectives, (2) optimized balance among quality assurance costs, schedules, and risk factors, and (3) the applicable system life cycle phases.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Work Breakdown Structure (WBS) (d) Customer's Statement of Work (SOW) (e) Contractor's proposal and subcontractor RFP/SOW (f) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Integrated Master Plane (IMP) (c) Integrated Master Schedule (IMS) (d) System Safety Program Budget Plan	(a) The contractor's internal System Safety Program Command Media should include a product unit-value/criticality versus System Safety Program capability level matrix. (b) The contractor's internal System Safety Program Command Media also should include a product life cycle versus System Safety Program capability level activities matrix. (c) All QA activities that can be "notionally" scheduled should be included in the Integrated Master Schedule (IMS). The rest of the activities should be allocated a fixed number of hours (i.e., Level of Effort) based on "estimated/anticipated" project support needs.
	2		**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW)	(a) SSPP includes a requirement versus task matrix that identifies all of the tasks that system safety will perform to achieve their system safety requirements.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
		Master Schedule (IMS), along with their key inputs and outputs/artifacts.	(d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (i) System Safety Program Plan and System Safety Working Group (SSWG) charter (j) Systems Engineering Management Plan (SEMP) (k) Integrate Master Plan (IMP) (l) Risk Management Plan (m) Quality Improvement Plan (n) System Safety Program Plan **(o)** RMAD Program Plan **(p)** End of Life Plan (EOLP)	(b) SSPP also includes a task versus performing discipline matrix that identifies all of the system safety tasks that other disciplines in Systems Engineering are responsible for performing. (c) Each discipline is supposed to have a similar matrix in their respective Plan to identify their applicable system safety tasks.
	2	All subcontractor key system safety data products/deliverables are identified in the SSPP.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) SEMP (c) IMP (d) Integrated Master Schedule (IMS)	(a) The SSPP should identifies the subcontractor's system safety data products/deliverables and their respective required delivery dates. (b) The SEMP and IMP should also identify the subcontractor's system safety data products/deliverables (c) The IMS should also identify the respective required delivery dates.
	2	All planned and LOE system safety tasks are adequately funded.	**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) System Safety Program Plan and System Safety Working Group (SSWG) charter (c) Individual Systems Engineering Discipline Plans **OUTPUTS:** (a) Integrated Master Schedule (IMS) (b) System Safety Program Budget Plan	(a) The SSPP identifies all scheduled and LOE system safety tasks. (b) The hours for the scheduled tasks are identified in the IMS. (c) The rationale for the fixed hours for each LOE task is documented in the System Safety Program Budget Plan. (d) The System Safety Program Budget Plan should show adequate funding for all of the QA tasks.
	3	The use of industry-acknowledged engineering/analytical methods is called out in the Plan of each discipline that is responsible for performing or supporting a system safety engineering/analytical task.	**INPUTS:** (a) Military and Commercial Standards and Guides (b) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (c) Individual Systems Engineering Discipline Plans	(a) Contractor's Internal System Safety Program Command Media requires all systems engineering disciplines to use validated analytical methods (b) Systems engineering disciplines should include in their respective plans the intent to use only validated analytical methods (c) Systems engineering disciplines identify all key assumptions in their analytical reports.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
	3	Plans are developed for safe disposal of hazardous materials and of the system itself during the post operational mission.	**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) System Safety Program Plan (SSPP) and System Safety Working Group (SSWG) charter (c) End of Life Plan (EOLP)	(a) The SSPP identifies the system's post-mission end of life (EOL) requirements that impact sysjtem safety. (b) The SSPP also identifies system safety as the coordinator of the development of the End of Life Plan (EOLP) (c) The EOLP should comply with its required format and address all of the EOL requirements
	4 & 5	A plan is developed and implemented to improve the safety design of the operational system over time.	**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) Project Quality Improvement Plan (b) Integrated Master Schedule (IMS) (c) FRACAS Plan (d) FRB Charter	(a) The SSPP identifies the system's quality improvement requirements. (b) The SSPP also identifies the Project Quality Improvement Plan development and implementation tasks. (c) The Project Quality Improvement Plan should comply with its required format and address all of the safety design improvement requirements. (d) The schedule for implementing the Project Quality Improvement Plan should be identified in the IMS. (e) The FRACAS and the FRB play crucial roles in identifying and mitigating safety design defects. Those roles should be defined in the FRACAS Plan and FRB Charter.
Program Coordination	1	System safety participates in all program meetings/reviews run by other disciplines in which decisions are made that impact the product's safety design. NOTE: These meetings include Failure Review Board (FRB) meetings and Configuration Control Board (CCB) meetings.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans	(a) All of the system safety requirements and their sources are identified in the Requirements vs. Tasks Matrix in the SSPP. (b) SSPP includes a requirement versus responsible discipline matrix that identifies all of the system safety requirements that other disciplines in Systems Engineering have. Each discipline is supposed to have a similar matrix in their respective Plan. These Plans are supposed to identify the tasks that will be performed to achieve the system safety requirements, and the intent to invite system safety to all meetings involving product safety.
	1	System safety coordinates meetings with other disciplines to plan and track the exchange of data products (i.e., giver and receiver) for shared program tasks (e.g., trade studies) and shared customer submittals.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW	(a) All of the system safety tasks and the requirements they address are identified in the Requirements vs. Tasks Matrix in the SSPP. (b) SSPP includes a tasks versus responsible discipline matrix that identifies all of the system safety tasks that other disciplines in Systems

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			(e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Individual Systems Engineering Discipline Plans	Engineering are responsible for performing Each discipline is supposed to have a similar matrix in their respective Plan. These Plans are supposed to identify the tasks that will be performed to achieve the system safety requirements, and the intent to invite system safety to all meetings involving product safety.
	1	System safety coordinates timely completion of systems engineering activities that must be performed in order to obtain the required safety certifications.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Military and Commercial QA Standards (d) Customer's Statement of Work (SOW) (e) Contractor's proposal and subcontractor RFP/SOW (f) Contractor's Internal System Safety Program Command Media (g) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) Individual Systems Engineering Discipline Plans (b) System Safety Working Group (SSWG) Meeting Minutes	(a) The SSPP identifies all of the required safety certifications and the disciplines that participate in obtaining them. (b) The Lead System Safety Engineer ensures that the required safety certifications are included in the Plan of each participating discipline. (c) The Lead System Safety Engineer periodically convenes System Safety Working Group (SSWG) meetings to ensure that a collaborative effort is implemented to obtain the required safety certifications.
	2	The Lead System Safety Engineer tracks the status of engineering/analytical reports and customer deliverables that system safety shares responsibility for with other disciplines.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media (f) System Safety Program Plan and System Safety Working Group (SSWG) charter (g) Individual Systems Engineering Discipline Plans **OUTPUTS:** (a) System Safety Working Group (SSWG) Meeting Minutes	(a) All of the system safety reports and their source requirement documents are identified in the Requirements vs. Tasks Matrix in the SSPP. (b) SSPP includes a tasks versus responsible discipline matrix that identifies all of the system safety related reports that other disciplines in Systems Engineering must generate. Each discipline is supposed to have a similar matrix in their respective Plan. (c) The System Safety Engineer periodically convenes System Safety Working Group (SSWG) meetings to ensure that a collaborative effort is implemented to generate reports and customer deliverables that are shared with other disciplines.
	2	System safety inputs to key project documents are properly reviewed, coordinated, and approved.	**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) Product Specifications (b) Calibration Standards (c) Production Procedures (d) Inspection Procedures	(a) All key project documents that require system safety inputs are identified in the SSPP (b) Each project document for which system safety provides a significant input is supposed to have an approval page with a signature line for the Lead System Safety Engineer.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
	2	The Lead System Safety Engineer monitors the system safety activities of subcontractors during product design, manufacture, assembly, test, inspection, shipping, and operations.	**INPUTS:** (a) Contractor's proposal and subcontractor RFP/SOW (b) Contractor's Internal System Safety Program Command Media (c) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) System Safety Working Group (SSWG) Meeting Minutes	(a) All of the subcontractor system safety requirements and tasks are identified in the SSPP. (b) The Lead System Safety Engineer periodically convenes System Safety Working Group (SSWG) meetings to ensure that subcontractors are properly implementing their required system safety tasks.
	3	All system safety stake-holders are identified and provided with applicable Safety Design Checklists to aid their mishap prevention activities.	**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) Mishap Prevention Checklists	(a) The SSPP should identify all of the Systems Engineering disciplines that have system safety responsibilities. (b) The SSPP should identify the development and distribution of system safety checklists as tasks. (c) The Lead System Safety Engineer coordinates the documentation, approval, and distribution of mishap prevention checklists.
	3	The contractor establishes and maintains a program-wide Hazard Tracking Log Database.	**INPUTS:** (a) SEMP (b) IMP (c) Contractor's Internal System Safety Program Command Media (d) System Safety Program Plan and System Safety Working Group (SSWG) charter (e) Individual Systems Engineering Discipline Plans **OUTPUTS:** (a) Systems Engineering Database	(a) The SEMP, IMP, and SSPP define the program-wide Hazard Tracking Log database purpose, structure, and data fields. (b) The Plans of various disciplines identify their data entries in the Hazard Tracking Log database.
	3	System safety collects, reviews, and utilizes safety design lessons learned, as applicable, and ensures that other disciplines also collect and utilize safety design lessons learned to help identify existing and potential hazards early. NOTE: These lessons learned include design, test, and operating guidelines.	**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) System Safety Program Plan and System Safety Working Group (SSWG) charter (c) Individual Systems Engineering Discipline Plans **OUTPUTS:** (a) Lessons Learned Review Committee (LLRC) Meeting Minutes (b) Lessons Learned Report	(a) The SEMP, IMP, and SSPP describe the program-wide Lessons Learned process (b) The Lessons Learned Report describes the new Lessons Learned records that were approved since the last publication. (c) Quality assurance is the administrator of the program-wide Lessons Learned process and coordinates the Lessons Learned Review Committee (LLRC).
	3		**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) System Safety Program Plan and System Safety Working Group (SSWG) charter (c) Individual Systems Engineering Discipline	(a) The SEMP, IMP, and SSPP describe the program-wide Lessons Learned process. (b) The SSPP and individual Plans of other Systems Engineering discipline should call out lesson learned identification as a key task. (c) System safety and the other systems engineering

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
		Failure/Discrepancy Reports.	Plans (d) Failure Reports (e) FRB Meeting Minutes **OUTPUTS:** (a) Lessons Learned Review Committee (LLRC) Meeting Minutes (b) Lessons Learned Report	disciplines submit new lessons learned to the Lessons Learned Review Committee (LLRC) for approval
	3	The Lead System Safety Engineer chairs system safety working group (SSWG) meetings with peers on a regular basis to review system safety reports and mitigate or control identified hazard risks and existing problems.	**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) System Safety Program Plan and System Safety Working Group (SSWG) charter (c) Production/Build Records **OUTPUTS:** (a) System safety working group (SSWG) meeting minutes.	(a) The Lead System Safety Engineer monitors all program-wide system safety activity and convenes SSWG meetings on an as needed basis to review system safety reports and disposition high and serious hazard risks. (b) All of the action items that come out of an SSWG meeting are supposed to be documented and tracked until closure.
	4 & 5	The Lead System Safety Engineer ensures all system safety stake-holders are trained to properly utilize the Safety Design Checklists that they are provided with.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) Contractor's Internal System Safety Program Command Media (c) System Safety Program Plan and System Safety Working Group (SSWG) charter (d) Individual Systems Engineering Discipline Plans **OUTPUTS:** (a) System Safety Training Materials	(a) All of the system safety tasks are identified in the SSPP along with the disciplines responsible for performing them. (b) The guidance for performing each system safety task should be provided in by some type of System Safety training materials.
Engineering & Evaluation	1	System safety reviews the detailed functional diagram models in the design specifications and FMECA Reports to ensure they accurately represent the required safety design functions. NOTE: This includes software logic flow diagram models in software component specifications.	**INPUTS:** (a) Design Specifications (b) FMECA Report **OUTPUT:** (a) Safety Assessment Report (SAR)	(a) System safety provides comments to the creators of functional diagram models via the Comment Resolution Matrix (CRM) on an as needed basis. (b) The Lead System Safety Engineer puts functional diagram models that accurately represent safety design functions in the Safety Assessment Report (SAR).
	1	The system's unacceptable fault/failure conditions are clearly defined. NOTE: These include unacceptable software safety design conditions, such as, safety-critical single-point-failure-mode software switching functions.	**INPUT:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) System Specification (e) FMECA Report (f) Anomaly Detection and Response (ADR) Design Specification **OUTPUT:** (a) Safety Assessment Report (SAR)	(a) The FMECA Report and ADR Design Specification are supposed to identify all of the system's unacceptable fault/failure conditions. (b) The Safety Assessment Report (SAR) is supposed to identify the system's unacceptable fault/failure conditions which may impact system safety.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
	1	A collaborative Preliminary Hazard List (PHL) is developed which identifies all known safety critical hardware, software, and procedures, and documents them in the initial Critical Items List (CIL), along with the appropriate controls for each. NOTE: This includes historical mishaps that were caused by operating software faults.	**INPUTS:** (a) Historical Field Failure Reports (b) Historical Test Discrepancy Reports (c) Lessons Learned (d) Historical FMECA Reports (e) Historical Reliability Prediction Reports (f) Historical Hazard Reports (g) Historical Safety Assessment Reports (SARs) **OUTPUT:** (a) Preliminary Hazard List (PHL) (b) Initial Critical Items List (CIL)	(a) The identification criteria for safety-critical items are supposed to be defined in the SOW and the contractor's internal System Safety Program Command Media. (b) The PHL is supposed to be developed from historical hazard and mishap information. (c) The initial CIL is supposed to be developed from historical FMECA reports, historical Hazard Reports, and historical Safety Assessment Report (SAR). (d) The PHL and initial CIL are documented, approved, maintained, and updated as needed.
	1	System safety performs a Requirements/Criteria Hazard Analysis (RHA-Task 203) .	**INPUTS:** (a) System Specifications (b) Preliminary Hazard List (PHL) (c) Lessons Learned **OUTPUTS:** (a) Requirements/Criteria Hazard Analysis (RHA)	(a) The Requirements/Criteria Hazard Analysis (RHA) is developed from fault/failure models of the system's functional and design specifications/requirements. (b) The PHL is input to the RHA, and vice versa. (c) The RHA is documented, approved, maintained, and updated as needed.
	1	System safety determines or obtains the engineering-estimate-based qualitative probability of occurrence for each safety critical function. NOTE: This includes engineering-estimate-based qualitative software probability of failure.	**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) Reliability Prediction Handbooks (e) FMECA Report (f) Component Reliability Prediction Reports (g) Test Discrepancy Reports **OUTPUT:** (a) Hazard Analysis Reports	(a) The approach for determining the engineering-estimate-based qualitative probability of occurrence for each safety critical function is supposed to be defined in the SOW and the contractor's internal System Safety Program Command Media. (b) The qualitative probability of occurrence is derived from reliability prediction handbooks, reliability prediction reports, FMECA reports, or test discrepancy reports. (c) The qualitative probabilities of occurrence for safety critical functions are documented in the hazard analysis reports.
	2	System safety evaluates all identified differences between (1) the build-to and as-built configurations of safety critical components, and (2) the qualification test and acceptance test of safety critical components.	**INPUTS:** (a) Engineering Change Proposal (ECP) **OUTPUT:** (a) Risk Submittal	(a) System safety reviews the ECPs for all safety critical components to identify and evaluate possible differences between (1) their build-to and as-built configurations, and (2) their qualification test and acceptance test. (b) Significant differences that affect the product's form, fit, or function are documented as risk submittals
	2		**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media	(a) The safety design criteria are supposed to be defined in the SOW and the contractor's internal System Safety Program Command Media. (b) FMECA reports, reliability prediction report, and other mission assurance reports identify the system's design faults and failure modes

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
		conditions.	(d) FMECA Reports (e) Reliability Prediction Reports (f) EMC Analysis Reports (g) Structural Analysis Reports (h) Thermal Analysis Reports **OUTPUTS:** (a) Hazard Reports	(c) System safety identifies the subset of all identified design faults and failure modes that also violate the safety design criteria. (d) The unacceptable safety design conditions are supposed to be documented in hazard reports.
	2	System safety performs a Preliminary Hazard Analysis (PHA- Task 202). NOTE: This includes the responsible Software Engineer performing a preliminary software hazard analysis based on the logic flow diagrams of the safety-critical software functions identified in the software/hardware interface FMECA.	**INPUTS:** (a) System Specifications (b) Preliminary Hazard List (PHL) (c) Test Discrepancy Reports (d) Lessons Learned (e) FMECA Reports (f) Reliability Prediction Reports **OUTPUTS:** (a) Preliminary Hazard Analysis (PHA)	(a) The Preliminary Hazard Analysis (PHA) is developed from the Preliminary Hazard List (PHL) and other systems engineering fault/failure reports. (b) Hardware and software hazards that may occur during the useful life of the system are collaboratively identified by the contractor's systems engineering disciplines. (c) The PHA is documented, approved, maintained, and updated as needed.
	2	System safety provides or obtains the handbook-based quantitative probability of occurrence for each safety critical function. NOTE: This includes engineering-estimate-based qualitative software probability of failure.	**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (c) Contractor's Internal System Safety Program Command Media (d) Reliability Prediction Handbooks (e) FMECA Report (f) Component Reliability Prediction Reports (g) Test Discrepancy Reports **OUTPUT:** (a) Hazard Analysis Reports	(a) The approach for determining the handbook-based quantitative probability of occurrence for each safety critical function is supposed to be defined in the SOW and the contractor's internal System Safety Program Command Media. (b) The handbook-based quantitative probability of occurrence is derived from reliability prediction handbooks, or obtained from reliability prediction reports or FMECA reports. (c) The handbook-based quantitative probabilities of occurrence for safety critical functions are documented in the hazard analysis reports.
	3	The Lead System Safety Engineer ensures that validated checklists and lessons learned are used by system safety stakeholders across the systems engineering process to help prevent mishaps from occurring. NOTE: This includes software design rules.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) Contractor's Internal System Safety Program Command Media (c) System Safety Program Plan and System Safety Working Group (SSWG) charter (d) Individual Systems Engineering Discipline Plans (e) Individual Systems Engineering Discipline Reports (f) System Safety Checklists (g) Lessons Learned Reports (with System Safety Lessons Learned identified) **OUTPUTS:** (a) System Safety Program Status Reports	(a) The requirement to use validated system safety checklists is found in the AIAA Mission Assurance Standards, and also should be found in the contractor's internal System Safety Program Command Media, the SSPP, and the plans and reports of other disciplines. (b) All of the system safety tasks are identified in the SSPP along with the disciplines responsible for performing them. (c) System safety should generate a checklist for each system safety task. (d) System safety should monitor the activities of system safety stakeholders, and report when they start and finish using a system safety checklist in the System Safety Program Status Report.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
	3	System safety performs a Subsystem Hazard Analysis (SSHA - Task 204).	**INPUTS:** (a) System Specifications (b) Preliminary Hazard Analysis (PHA) (c) Test Discrepancy Reports (d) Lessons Learned (e) FMECA Reports (f) Reliability Prediction Reports **OUTPUT:** (a) Subsystem Hazard Analysis (SSHA)	(a) The Subsystem Hazard Analysis (SSHA) is developed from the Preliminary Hazard Analysis (PHA) and other systems engineering fault/failure reports. (b) Hardware and software hazards that may occur during the useful life of the subsystem are collaboratively identified by the contractor's systems engineering disciplines. (c) The SSHA is documented, approved, maintained, and updated as needed.
	3	System safety performs a System Hazard Analysis (SHA - Task 205).	**INPUTS:** (a) System Specifications (b) Preliminary Hazard Analysis (PHA) (c) Test Discrepancy Reports (d) Lessons Learned (e) FMECA Reports (f) Reliability Prediction Reports **OUTPUT:** (a) Subsystem Hazard Analysis (SSHA)	(a) The System Hazard Analysis (SHA) is developed from the Preliminary Hazard Analysis (PHA), SSHA, and other systems engineering fault/failure reports. (b) Hardware and software hazards that may occur during the useful life of the system are collaboratively identified by the contractor's systems engineering disciplines. (c) The SHA is documented, approved, maintained, and updated as needed.
	3	System safety provides or obtains the field-failure-based, test-failure-based, or stress-based fault/failure distribution estimate for each safety critical function. NOTE: This includes the estimated software initial failure rate based on in-house software qualification testing.	**INPUTS:** (a) Customer's Statement of Work (SOW) (b) Contractor's proposal and subcontractor RFP/SOW (h) Contractor's Internal System Safety Program Command Media (i) Reliability Prediction Guides (j) FMECA Report (k) Component Reliability Prediction Reports (l) Test Discrepancy Reports **OUTPUT:** (a) Hazard Analysis Reports	(a) The approach for determining the field-failure-based, test-failure-based, or stress-based quantitative probability of occurrence for each safety critical function is supposed to be defined in the SOW and the contractor's internal System Safety Program Command Media. (b) The field-failure-based, test-failure-based, or stress-based quantitative probability of occurrence is derived from reliability prediction guides, or obtained from reliability prediction reports or FMECA reports. (c) The field-failure-based, test-failure-based, or stress-based quantitative probabilities of occurrence for safety critical functions are documented in the hazard analysis reports.
	4 & 5	System safety performs an Operating and Support Hazard Analysis (O&SHA - Task 206).	**INPUTS:** (a) System Specifications (b) Preliminary Hazard Analysis (PHA) (c) Test Discrepancy Reports (d) Lessons Learned (e) FMECA Reports (f) Reliability Prediction Reports **OUTPUT:** (a) Operating and Support Hazard Analysis (O&SHA)	(a) The Operating and Support Hazard Analysis (O&SHA) is developed from the Preliminary Hazard Analysis (PHA) and other systems engineering fault/failure reports. (b) Procedure hazards that may occur during the useful life of the system are collaboratively identified by the contractor's systems engineering disciplines. (c) The O&SHA is documented, approved, maintained, and updated as needed.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
	4 & 5	The input data and assumptions that are utilized in all system safety engineering and analytical methods are identified and evaluated with regard to their maturity. NOTE: This includes the assumed software reliability growth rate at time of delivery.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) Contractor's Internal System Safety Program Command Media (c) Individual Systems Engineering Discipline Plans **OUTPUT:** (a) Systems Engineering Discipline Analytical Reports	(a) Contractor's System Safety Program Command Media requires all systems engineering disciplines to evaluate the maturity of the input data and assumptions that are utilized in all system safety engineering and analytical methods for high unit-value/criticality products. (b) The analytical reports of the various systems engineering disciplines should identify the maturity of the input data and assumptions used for each system safety engineering and analytical method. (c) The system safety engineering and analytical reports of the various systems engineering disciplines should also identify any uncertainties associated with the input data.
	4 & 5	System safety ensures that validated computer-aided mission assurance tools are acquired and integrated to the greatest extent practical to form a comprehensive system safety toolset.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) Contractor's Internal System Safety Program Command Media (c) Individual Systems Engineering Discipline Plans **OUTPUT:** (a) Systems Engineering Discipline Analytical Reports	(a) Contractor's System Safety Program Command Media requires that validated computer-aided mission assurance tools be acquired and integrated to the greatest extent practical to form a comprehensive system safety toolset for very-high unit-value/criticality products. (b) The analytical reports of the various systems engineering disciplines should identify the validated computer-aided system safety tools that were used.
Risk Assessment & Tracking	1	The hazard risk mitigation/control order of precedence is implemented in accordance with the MIL-STD-882C order of precedence and enforced across the systems engineering process.	**INPUTS:** (d) AIAA Standard S-102.0.1 (a) MIL-STD-882D (b) AFI 91-202 AFSPC SUP1 (c) AFI 91-217 (d) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Risk Management Plan (RMP) (c) Failure Review Board (FRB) Charter (d) Configuration Control Board (CCB) Charter	(a) Contractor's internal System Safety Program Command Media requires using the risk and problem mitigation order of precedence that is consistent with AIAA Standard S-102.0.1, MIL-STD-882C, AFI 91-202 AFSPC SUP1, and AFI 91-217. (b) The contractor's SSPP, Risk Management Plan (RMP), FRB charter, and CCB charter should all define a risk/problem mitigation order of precedence that is consistent with AIAA Standard S-102.0.1 and MIL-STD-882C.
	1	The mitigation/control approaches that are chosen for identified hazard risks are all tracked to closure.	**INPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Risk Management Plan (RMP) (c) Failure Review Board (FRB) Charter (d) Configuration Control Board (CCB) Charter (e) FMECA Report (f) Worst Case Analysis Report	(a) The contractor's SSPP, SSWG Charter, Risk Management Plan, and other Plans, should describe the process for tracking and resolving concerns that are identified in analytical reports. (b) The contractor's Risk Management Database Report and the Hazard Tracking Log Database should identify the concerns that are being tracked.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			(g) Parts Stress Derating Analysis Report (h) Circuit Thermal Stress Analysis Report (i) Circuit Structural Stress Analysis Report **OUTPUTS:** (a) Risk Management Database Report (b) Hazard Tracking Log Database	
	1	All high and serious hazard risks are reported to the proper risk acceptance authority and appropriately adjudicated.	**INPUTS:** (a) Contractor's Internal System Safety Program Command Media (b) Individual Systems Engineering Discipline Plans (c) System Safety Program Plan and System Safety Working Group (SSWG) charter (d) Risk Management Plan (RMP) (e) Failure Review Board (FRB) Charter (f) Configuration Control Board (CCB) Charter **OUTPUTS:** **(a)** Risk Management Database Report **(b)** Hazard Tacking Log Database	(a) The contractor's internal System Safety Program Command Media should include a requirement to identify all high and serious hazard risks. (b) The contractor's SSPP and Risk Management Plan (RMP) should also include a requirement to identify all high and serious hazard risks. (c) The high and serious hazard risks should be identified in the Risk Management Database Report and the Hazard Tracking Log Database.
	2	The risk metrics that are used across systems engineering complies with the safety critical risk metrics and the mission critical risk metrics, in that order of precedence.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) System safety Program Plan (SSPP) (c) RMAD Program Plan (d) Risk Management Plan (RMP)	(a) The safety critical risk metrics definitions and the mission critical risk metrics risk metrics definitions should be defined in the SOW and the contractor's System Safety Program Command Media. (b) The contractor's SSPP, RMAD Program Plan, and Risk Management Plan should all define the order of precedence of risk metrics to be safety critical risk metrics, and mission critical risk metrics, in that order.
	3	The Lead System Safety Engineer convenes System Safety Working Group (SSWG) meetings with peers on a regular basis to review identified hazard risks and choose the appropriate mitigates or controls.	**INPUT:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUT:** (a) System Safety Working Group Meeting Minutes	(a) The SSWG Charter should call for the Lead Quality Engineer to convene SSWG meetings with peers on a regular basis to mitigate or control hazard risks and correct system safety problems. (b) The SSWG meeting minutes should identify the new action items and the status of all the old action items that have not been closed.
	3	The Lead System Safety Engineer ensures that all requests for a requirement waiver involving a safety critical hazard include evidence that the level of hazard risk is acceptable.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's Internal System Safety Program Command Media (e) System Safety Program Plan (SSPP)	(a) The contractor's internal System Safety Program Command Media should require that all requests for a requirement waiver involving a safety critical hazard include evidence that the level of hazard risk is acceptable. (b) The acceptable risk criteria should be identified in the SSPP, RMAD Program Plan, SSPP, and Risk

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			(f) RMAD Program Plan (g) System Safety Program Plan and System Safety Working Group (SSWG) charter (h) Risk Management Plan (i) Waiver Request **OUTPUTS:** (a) Risk Submittal	Management Plan. (c) System safety should evaluate the Waiver Request, and if necessary, generates a Risk Submittal. (d) The Risk Submittal should identify the residual risk associated with the Waiver Request.
	4 & 5	The Lead System Safety Engineer periodically inspects/audits various systems engineering disciplines (including system safety) to identify and mitigate/control latent hardware, software, process hazard risks early.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's Internal System Safety Program Command Media (e) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) System Safety Program Inspection/Audit Report	(a) The contractor's internal System Safety Program Command Media should require a periodic audit of various systems engineering disciplines. (b) The system safety inspection/audit criteria should be identified in the System Safety Program Command Media. (c) The SOW and SSPP may include requirements for the customer to periodically inspect/audit the contractor, or for the contractor to periodically inspect/audit the major subcontractors. (d) The results of the inspection/audit should be documented in the System Safety Program Inspection/Audit Report.
	4 & 5	Overlooked, missing, or deficient system safety tasks are identified, assessed for residual risk, and those found to be unacceptable are reported to the appropriate risk acceptance authority for adjudication.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Subcontractor SOW (e) Contractor's Internal System Safety Program Command Media (f) System Safety Program Plan and System Safety Working Group (SSWG) charter (g) Risk Management Plan (RMP) **OUTPUT:** (a) Requirements Hazard Analysis Report	(a) AIAA Standard S-102.0.1, MIL-STD-882C, the SOW, the subcontractor SOW, and the contractor's internal System Safety Program Command Media aid the identification of all required system safety tasks. (b) The contractor's internal System Safety Program Command Media should include a requirement to identify overlooked, missing, or deficient system safety engineering and testing tasks. (c) The contractor's SSPP and Risk Management Plan (RMP) should include tasks to identify overlooked, missing, or deficient system safety engineering and testing tasks. (d) The Requirements Hazard Analysis Report should identify overlooked, missing, or deficient system safety engineering and testing tasks.
	4 & 5	The system safety 4x5 hazard risk matrix is translated to the conventional 5x5 risk matrix in a single program-wide risk management process.	**INPUTS:** (a) AIAA Standard S-102.0.1 (b) MIL-STD-882C (c) Customer's Statement of Work (SOW) (d) Contractor's proposal and subcontractor RFP/SOW (e) Contractor's Internal System Safety Program Command Media **OUTPUTS:** (a) System Safety Program Plan and System Safety	(a) The program-wide risk matrix format should be defined in the SOW and the contractor's System Safety Program Command Media. (b) The contractor's SSPP, RMAD Program Plan, and Risk Management Plan should all define the translation format for going from a 4x4 system safety risk matrix to a 5x5 convention risk matrix.

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			Working Group (SSWG) charter (b) RMAD Program Plan (c) Risk Management Plan (RMP)	
Verification (Including Product Safety Testing)	1	Special inspection or similarity checklist methods are used to verify the safety requirements and self-imposed objectives for safety-critical HW, SW, and procedures that are rated moderate hazard risks. This partially fulfills Safety Verification (Task 401)	**INPUTS:** (a) Product Specifications (b) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) SSWG Meeting Minutes (b) Test Plans (c) Test Reports	(a) The contractor's SSPP should identify the routine test methods used to verify that all safety-critical HW, SW, and procedures that are rated moderate hazard risks, comply with applicable military, federal, national, international, and industry quality standards and certifications. (b) The contractor's SSWG coordinates with Test Engineering to ensure cost-effective test methods are selected and implemented. (c) The Test Plans describe the routine test procedures. (d) The Test Reports provide the results of the routine test procedures.
	1	System safety evaluates and participates in the disposition of functional test discrepancies involving safety critical components.	**INPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Critical Items List (CIL) (c) Test Plans (d) Test Discrepancy Report **OUTPUTS:** (a) Failure Analysis Report (b) Failure Review Board (FRB) Meeting Minutes Report	(a) The contractor's SSPP should describe the process for evaluating and dispositioning the functional test discrepancies of all safety critical components. (b) The CIL identifies all safety critical components. (c) The Discrepancy Report describes the test discrepancy/failure events. (d) The Failure Analysis Report and FRB meeting minutes identify the failure root cause and corrective action.
	2	Special analysis or simulation methods are used to verify the system safety requirements and self-imposed objectives for safety critical components that are rated serious hazard risks. This objective partially fulfills Safety Verification. (MIL-STD-882C, Task 401)	**INPUTS:** (a) Product Specifications (b) Critical Items List (CIL) Report (c) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) Test Plans (b) Test Reports (c) SSWG Meeting Minutes Report	(a) The CIL should identify the special demonstrations, tests, inspections, analyses, simulations, and inspections used to verify safety-critical HW, SW, and procedures that are rated serious hazard risks, comply with system safety requirements and self-imposed objectives. (b) The SSWG coordinated with Test Engineering to ensure cost-effective test methods are selected and completed. (c) The Test Plans describe the special test procedures. (d) The Test Reports provide the results of the special test procedures.
	3	Special demonstration or test methods are used to verify the system safety requirements and self-imposed objectives for safety critical components that are rated high hazard risks. This objective partially fulfills Safety Verification. (MIL-STD-882C, Task 401)	**INPUTS:** (a) Product Specifications (b) Critical Items List (CIL) Report (c) System Safety Program Plan and System Safety Working Group (SSWG) charter **OUTPUTS:** (a) Test Plans	(a) The CIL should identify special demonstrations, tests, inspections, analyses, simulations, and inspections used to verify safety-critical HW, SW, and procedures that are rated high hazard risks, comply with system safety requirements and self-imposed objectives. (b) The SSWG coordinated with Test Engineering to

PROGRAM AREA	CAPABILITY LEVEL	OBJECTIVES	CANDIDATE ARTIFACTS	OUTPUT ARTIFACT EVALUATION CRITERIA
			(b) Test Reports (c) SSWG Meeting Minutes Report	ensure cost-effective test methods are selected and completed. (c) The Test Plans identify the special test procedures. (d) The Test Reports provide the results of the special test procedures.
	3	System safety reviews the reports of other disciplines to verify that industry acknowledged methods were use to perform their system safety related tasks. NOTE: This includes software test reports.	**INPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Plans of various Systems engineering disciplines. (c) Engineering/analytical reports of various Systems engineering disciplines. **OUTPUTS:** (a) System Safety Program Status Reports	(a) The SSPP should identify a requirement for the Lead System Safety Engineer to verify that industry acknowledged methods were use to perform all system safety related tasks performed by other disciplines. (b) SSPP includes a requirement versus responsible discipline matrix that identifies all system safety related tasks performed by other disciplines in systems engineering. Each discipline is supposed to have a similar matrix in their respective Plan. These Plans are supposed to identify the tasks that will be performed to achieve the system safety requirements. (c) System safety program status reports verify that industry acknowledged methods were use to perform all system safety related tasks.
	4 & 5	System safety verifies that the probability values generated for all high and serious hazard risks are obtained from statistical methods that provide lower bound confidence.	**INPUTS:** (a) System Safety Program Plan and System Safety Working Group (SSWG) charter (b) Plans of various Systems engineering disciplines. (c) Engineering/analytical reports of various Systems engineering disciplines. **OUTPUTS:** (a) System Safety Program Status Reports	(a) The SSPP should identify a requirement for the probability values generated for all high and serious hazard risks to be obtained from statistical methods that provide lower bound confidence. (b) SSPP includes a requirement versus responsible discipline matrix that identifies all system safety related tasks performed by other disciplines in systems engineering. Each discipline is supposed to have a similar matrix in their respective Plan. These Plans are supposed to identify the tasks that will be performed to achieve the system safety requirements. (c) System safety program status reports verify that the probability values generated for all high and serious hazard risks were obtained from statistical methods that provide lower bound confidence.

5.6 Hazard Risk Assessment and Tracking

SET will use the conventional 5x5 risk matrix to assess system safety risks. SET will present all high and serious hazard risks identified using the MIL-STD-882 system safety methodology in the format of the translation table shown in Figure 5.

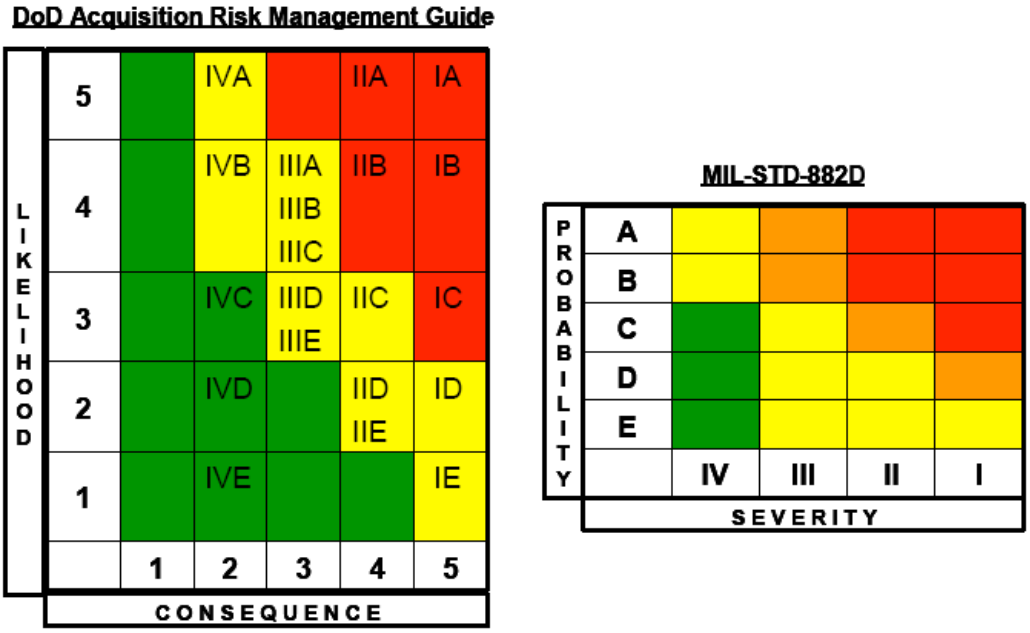

Figure 5: Translation of MIL-STD-882 Risk Matrix to the Conventional 5x5 Risk Matrix

5.7 Requirements Verification

System safety verifies that each system specification requirement has a corresponding Requirement Verification Plan (RVP) and Requirements Verification Reports (RVR). The SSPP should identify the system safety related RVPs and RVRs developed by other disciplines. The RVPs and RVRs are entered and maintained in the project-wide Systems Engineering Database.

5.7.1 Verify Use of Industry Acknowledged Engineering Methods

The Lead System Safety Engineer will verify industry acknowledged methods were use by systems engineering disciplines to perform their system safety related tasks. The engineering reports generated by these disciplines should include references to public domain documents that describe the basis for industry acknowledgement of the systems engineering methods used.

ANNEX A

1. Hazard Analysis

1.1 Purpose

The purpose of hazard analysis is to identify hazardous conditions/risks for the purpose of their elimination or control. A hazardous condition is a prerequisite to a mishap. Hazard analysis is performed to examine the system, subsystems, components, and their interrelationships, as well as logistic support, training, maintenance, operational environments, and system/component disposal plans to:

- Identify hazards and recommend appropriate corrective action.
- Assist the individual(s) actually performing the analysis in better evaluating the safety aspects of a given system or element.
- Provide managers, designers, test planners, and other affected decision makers with the information and data needed to permit effective tradeoffs.
- Demonstrate compliance with given safety-related technical specifications, operational requirements, and design objectives.

1.2 Process Description

The contractor shall assess the severity or magnitude, importance, and frequency or likelihood of the worst-case mishap caused by hazards at every system indenture level. This assessment involves determining the appropriate corrective action to eliminate or control unacceptable hazards and avoid postulated mishaps of catastrophic or critical severity levels. The hazard evaluation results shall be communicated in a timely manner to those individuals having the decision-making authority to implement corrective actions. Needed safety design changes shall be identified and completed early in the system's life cycle to minimize the impact on cost and schedule. Figure A-1 provides the applicability of Hazard Analysis in the product life cycle.

Figure A-1: Applicability of Hazard Analysis in Product Life Cycle.

S-102.2.14	Product Life Cycle Phase				
Product Unit Value	Conceptual Design Phase	Preliminary Design Phase	Detailed Design Phase	Fabrication, Assembly, Integration and Test	Delivered Product Operation & Service
Low Unit-Value	Capability Level 1 Activities	Capability Level 1 Activities	Capability Level 1 Activities	Capability Level 1 Activities	Capability Level 1 Activities (*)
Medium Unit-Value	Capability Level 1 Activities	Capability Level 2 Activities	Capability Level 2 Activities	Capability Level 2 Activities	Capability Level 2 Activities (*)
High Unit-Value	Capability Level 1 Activities	Capability Level 2 Activities	Capability Level 3 Activities	Capability Level 3 Activities	Capability Level 3 Activities (*)
Very-High Unit-Value	Capability Level 1 Activities	Capability Level 2 Activities	Capability Level 4 Activities	Capability Level 4 Activities	Capability Level 4 Activities (*)
Ultra-High Unit-Value	Capability Level 1 Activities	Capability Level 2 Activities	Capability Level 4 Activities	Capability Level 5 Activities	Capability Level 5 Activities (*)

(*) indicates that the process capability level activities only apply to changes that occur during that product life cycle phase.

ANNEX B

AIAA S-102 Hazard Analysis Capability Level Requirements (normative)

B.1 The Capability Level 1 Hazard Analysis Process shall include the following tasks at a minimum:

B.1.1 Timely establishment of the requirements and analytical ground-rules for the Hazard Analysis;

B.1.2 Timely establishment of the Hazard Analysis Technical Performance Metrics (TPMs);

B.1.3 Timely collection or development, as necessary, of the following system design and operating information to be used for the identification of unacceptable hazards in ground, sea, air, or space systems or fixed ground system, as applicable, which may lead to possible mishaps of catastrophic or critical severity:

- System design safety and safing requirements;
- System hierarchical functional flow for hardware components, subsystem-to-subsystem hardware interfaces, and redundant and standby hardware paths
- Mission description, including timeline for each mission phase
- Description of all system operating modes, including contingency and workaround modes, degraded operating modes, and scheduled maintenance
- Description of all hardware components and an indentured parts list
- Approved materials list
- Functional-to-physical association of all hardware components
- Environmental and operating stresses for each hardware component
- Product FMECAs
- Process FMECAs
- Reliability models and predictions
- System operating manuals and commands list
- System safing procedures
- Safety lessons learned pertinent to mishaps of similar systems caused by hardware component failures and drawing errors

B.1.4 Timely construction and documentation of the Preliminary Hazard List:

B.1.5 Timely performance and documentation of Requirements Hazard Analysis

- Analyze the system design requirements, system/segment specifications, preliminary hardware configuration item development specification, software requirements specifications, and the interface requirements specifications, as appropriate, to identify hazards

- Ensure that the system safety design requirements and guidelines are developed, refined, correctly and completely specified, properly translated into system hardware and software requirements and into operator, user's, and diagnostic manuals, where appropriate
- Identify safety-critical hardware and software functions, including control functions, monitoring functions, interlock functions, inhibiting, safing functions, and functions that indirectly impact system safety
- Ensure that safety design requirements are properly implemented in the design and development of the system hardware and associated software
- Ensure that safety-related testing requirements are properly incorporated into the hardware, software, and system test plans
- Ensure that safety criteria in the operations and human factors specification(s) have been satisfied
- Develop a method of verifying each safety design requirement, safety-related testing requirement, and safety criterion is met

B.1.6 Timely integration of the PHL results with the Requirements Hazard Analysis results, as appropriate

B.1.7 Timely documentation and reporting to the acquisition activity of all residual risks identified from the hazard analyses performed.

B.2 The Capability Level 2 Hazard Analysis Process shall include all the tasks in the Capability Level 1 Hazard Analysis Process plus the following at a minimum:

B.2.1 Timely collection or development, as necessary, of the following system design and operating information to be used for the identification of unacceptable hazards in ground, sea, air, or space systems or fixed ground system, as applicable, which may lead to possible mishaps of catastrophic or critical severity:

- Software safety design requirements
- System hierarchical functional flow for software components, subsystem-to-subsystem software interfaces, and redundant software paths
- Descriptions of all software components with associated logic diagrams
- Functional-to-functional association of all software/hardware component interfaces
- Safety lessons learned pertinent to mishaps caused by software anomalies
- Software test and field anomaly data
- Pertinent historical software safety experiences for similar systems

B.2.2 Timely development, documentation, and flow down, as appropriate, of a Hazard Analysis Plan that is based on industry-accepted concepts for performance-based practices and is an integral part of the System Safety Program Plan. The Hazard Analysis

Plan shall describe the scope, objectives, ground rules, assumptions, activities or approaches, tools to be used, data products, and the organizational elements responsible for generating and processing the Hazard Analysis data products.

B.2.3 Timely performance and documentation of the following Preliminary Hazard Analysis (PHA) activities:

- Review the test and field anomaly data of similar systems.
- Identify known system hardware hazards and determine the severity of the associated worst-case experienced or postulated mishaps
- Develop a categorized list of basic energy sources.
- Investigate the various energy sources to determine the provisions which have been developed for their control.
- Identify safety design requirements and other regulations pertaining to system safety, personnel safety, environmental hazards, and toxic/corrosive substances with which the system will have to comply.
- Utilize the Product FMECA to the greatest extent practical to identify Severity Level I and II hazards
- As part of PHA, identify known software life cycle hazards and determine the severity of the associated worst-case experienced or postulated mishaps
- As part of PHA, identify known causes of human errors and determine the severity of the associated worst-case experienced or postulated mishaps
- Identify and recommend appropriate corrective actions, using the system safety precedence, to eliminate or reduce the risk of possible catastrophic and critical mishaps due to one or multiple hazards
- Track until closure the approved corrective actions to avoid the experienced and postulated catastrophic and critical mishaps

B.2.4 Timely integration of the PHA results with the Requirements Hazard Analysis results, as appropriate

B.3 The Capability Level 3 Hazard Analysis Process shall include all the tasks in the Capability Level 2 Hazard Analysis Process plus the following at a minimum:

B.3.1 Timely collection or development, as necessary, of the following system design and operating information to be used for the identification of unacceptable hazards in ground, sea, air, or space systems or fixed ground system, as applicable, which may lead to possible mishaps of catastrophic or critical severity:

- Human factors engineering data, including operating constraint requirements, cockpit requirements, as applicable, and system and interface requirements provided by pilots who use the system
- Operator/user personnel qualification requirements

- Safety lessons learned pertinent to mishaps caused by ambiguous procedures and human error

B.3.2 Timely performance and documentation of the following Subsystem Hazard Analysis (SSHA) activities:

- Review the test and field anomaly data of similar subsystems
- Identify the safety design criteria for hardware components and verify they have been satisfied
- Analyze the subsystem and each component to identify hazards associated with undesired operating modes which may lead to catastrophic or critical mishaps
- Utilize the Product FMECA to the greatest extent practical to identify the modes of failure of components, including human errors, and their effects on the safety of the subsystem
- Analyze multiple component failure modes and multiple undesired operating modes, in accordance with requirements, to determine the effects on System Safety with regard to possible catastrophic or critical mishaps
- Use Fault Tree Analysis or similar methodology to evaluate fault tolerance/redundancy of safety-critical functions
- As part of SSHA, identify the potential contribution of subsystem software events, faults, and occurrences (such as improper timing) on the safety of the subsystem
- Identify and recommend appropriate corrective actions, using the system safety precedence, to eliminate or reduce the risk of possible catastrophic and critical mishaps due to one or multiple hazards
- Track until closure the approved corrective actions to avoid the postulated catastrophic and critical mishaps
- Integrate the SSHA results with the PHA results and the Requirements Hazard Analysis results, as appropriate

B.3.3 Timely performance and documentation of the following System Hazard Analysis (SHA) activities:

- Determine that the safety design criteria in the subsystem interface specification(s) have been satisfied
- Analyze each subsystem-to-subsystem interfaces and identifying hazards associated with failure modes and undesired operating modes
- Analyze each subsystem-to-subsystem interface failure mode or undesired operating mode to determine the effects on System Safety with regard to possible catastrophic or critical mishaps throughout the system lifecycle, including its proper disposal
- Utilize the Product FMECA to the greatest extent practical to identify the modes of failure of components, including human errors, and their effects on the safety of the system

- Analyze multiple subsystem-to-subsystem interface failure modes and undesired operating modes, in accordance with requirements, to determine the effects on System Safety with regard to possible catastrophic or critical mishaps throughout the system lifecycle, including its proper disposal
- Use Fault Tree Analysis or similar methodology to evaluate fault tolerance/redundancy of safety-critical functions. Identify propagating, dependent, and simultaneous hazardous events, including failure modes of safety devices and common cause failure modes that could create a hazard.
- As part of SHA , identify the potential contribution of system software events, faults, and occurrences (such as crashes) on the safety of the system
- Identify and recommend appropriate corrective actions, using the system safety precedence, to eliminate or reduce the risk of possible catastrophic and critical mishaps due to one or more hazards
- Track until closure the approved corrective actions to avoid the postulated catastrophic and critical mishaps
- Integrate the SHA results with the PHA results, the SSHA results, and the Requirements Hazard Analysis results, as appropriate

B.3.4 Timely development and maintenance of a Hazard Report Database that is compatible with the Product FMECA/Hazards Analysis database and can automatically generate the Hazard Analysis Report

B.3.5 Timely utilization of Hazard Analysis results/data to the greatest extent practical by project functions, such as, Design, Logistics, Risk Management, Test, Operations Planning, and R&M Program tasks, such as, Product FMECA and FRACAS, to aid in minimizing the likelihood of broad categories of system mishaps as part of the overall System Safety effort. The exchange of Hazard Analysis data products shall be based on the established Systems Engineering data flow schemas for all applicable product development phases

B.3.6 Timely collection and review of existing Hazard Analysis lessons learned that are: (1) derived from sources internal to the enterprise, and (2) relevant to the system being developed. The objective of this activity is to identify needed Hazard Analysis process improvements.

B.3.7 Timely evaluation of all aspects of the Hazard Analysis process, including its implementation and data products, to identify candidate product-based and process-based lessons learned candidates. Evaluate for quality and prioritize these candidate lessons learned, and forward them to the Lessons Learned Approval Authority for appropriate action.

B.4 The Capability Level 4 Hazard Analysis Process shall include all the tasks in the Capability Level 3 Hazard Analysis Process plus the following at a minimum:

B.4.1 Timely performance and documentation of the following Operating and Support Hazard Analysis (O&SHA) activities:

- Identify hazards associated with component level and above testing, installation, modification, maintenance, transportation, and storage,
- Identify hazards associated with ground servicing
- Identify hazards associated with operations
- Identify hazards associated with, emergency escape, egress, rescue, and post-accident responses
- Identify hazards associated with training and rehearsals
- Identify hazards associated with supporting tools or other equipment, including software-controlled automatic test equipment
- Identify hazards associated with the effects and limitations of procedures, task sequences, and concurrent tasks
- Identify hazards associated with biotechnological factors
- Identify hazards associated with regulatory or contractually specified personnel safety and health requirements
- Identify hazards associated with potential unplanned events, including hazards introduced by human errors
- Utilize the Process FMECA to the greatest extent practical to identify Severity I and II hazardous operations
- Utilize Fault Tree Analysis or similar methodology to evaluate fault tolerance/redundancy of safety-critical operations
- As part of O&SHA, identify the potential contribution of operational or support software events, faults, and occurrences (such as command contention) on the safety of operations, support, and personnel
- Identify and recommend appropriate corrective actions, using the system safety precedence, to eliminate or reduce the risk of possible catastrophic and critical mishaps due to one or more hazards
- Track until closure the approved corrective actions to avoid the postulated catastrophic and critical mishaps
- Integrate the O&SHA results with the PHA results, the SSHA results, the SHA results, and the Requirements Hazard Analysis results, as appropriate

B.4.2 Timely performance and documentation of the Human Error Analysis that is performed on events, such as, safing, restoration, recovery, testing, installation, repair, maintenance (including Built-In Test), handling, transportation, storage, normal and contingency operations, rescue operations, post anomaly/accident/mishap responses, and disposal, to identify singular or multiple human errors, as applicable, which may cause catastrophic or critical mishaps

- Identify the potential contribution of human errors on the safety of the subsystem and system
- Identify the potential contribution of human errors on the safety of operations, support, and personnel
- As part of Human Error Analysis, identify the potential contribution of operational or support software events, faults, and occurrences (such as command contention) on the severity and frequency of human errors
- Integrate the Human Error Analysis results with the PHA results, the SSHA results, the SHA results, the O&SHA results, and the Requirements Hazard Analysis results, as appropriate

B.4.3 Timely development and maintenance of a Hazard Report Database that complies with the keyword data element descriptions (DEDs) in Annex C of this Standard

B.4.4 Timely evaluation of the Hazard Analysis data products in accordance with the Maturity Rating and Severity Classification scales defined in this Standard

B.4.5 Timely evaluation of the user-utility of the Hazard Analysis data products, by following up data transmittals with offers of aid to ensure proper use (For example, offer to assist users in interpreting Hazard Analysis data or explain the assumptions behind it.)

B.4.6 Timely exchange of Hazard Analysis lessons learned with other projects throughout the enterprise. Review the Hazard Analysis lessons learned that are received from other projects to identify needed process improvements, such as, improved procedures or training materials.

B.5 The Capability Level 5 Hazard Analysis Process shall include all the tasks in the Capability Level 4 Hazard Analysis Process plus the following at a minimum:

B.5.1 Timely development and implementation of a structured review process[3] (Independent Review Team/Panel, Independent Technical Assessment, etc.) that draws heavily on failure experiences of similar systems to aid the implementation or evaluation of the Hazard Analysis process, as appropriate, in all product life cycle development phases.

B.5.2 Timely establishment of a process for the continuous improvement of the enterprise approved Hazard Analysis practices and training materials. This activity includes annual

[3] The development and implementation of a comprehensive review checklist facilitates a structured review process.

goal setting and periodic independent evaluations of the organization's progress toward those goals.

B.5.3 Timely collection and review of Hazard Analysis lessons learned that are documented by outside organizations to identify significant recommendations that should be implemented by the project. Share Hazard Analysis lessons learned that are not subject to proprietary or legal constraints with external organizations through established channels, such as, the Government-Industry Data Exchange Program (GIDEP) or a non-profit research and development (R&D) consortium. (This activity requires establishing appropriate safeguards for security-classified, ITAR-restricted, and proprietary data).