TECHNICAL REPORT

GEIA-STD-0010	
Issued 2008-10	

Standard Best Practices for System Safety
Program Development and Execution

NOTICE

This document has been taken directly from the original TechAmerica document and contains only minor editorial and format changes required to bring it into conformance with the publishing requirements of SAE Technical Standards. The release of this document is intended to replace the original with the SAE International document. Any numbers established by the original document remain unchanged.

The original document was adopted as an SAE publication under the provisions of the SAE Technical Standards Board (TSB) Rules and Regulations (TSB 001) pertaining to accelerated adoption of specifications and standards. TSB rules provide for (a) the publication of portions of unrevised specifications and standards without consensus voting at the SAE committee level, and (b) the use of the existing specification or standard format.

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

SAE values your input. To provide feedback on this Technical Report, please visit
http://www.sae.org/technical/standards/GEIASTD0010

GEIA-STD-0010

TechAmerica Standard

Standard Best Practices for System Safety Program Development and Execution

GEIA-STD-0010

October 2008

TechAmerica
WHERE THE FUTURE BEGINS
THE ASSOCIATION OF COMPANIES DRIVING INNOVATION WORLDWIDE

NOTICE

TechAmerica Engineering Standards and Publications are designed to serve the public interest by eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards and Publications shall not in any respect preclude any member or nonmember of TechAmerica from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than TechAmerica members, whether the standard is to be used either domestically or internationally.

Standards and Publications are adopted by TechAmerica in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TechAmerica does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This TechAmerica Standard is considered to have International Standardization implications, but the ISO/IEC activity has not progressed to the point where a valid comparison between the TechAmerica Standard and the ISO/IEC document can be made.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(Formulated under the cognizance of the TechAmerica G-48 System Safety Committee).

This document is maintained under the ANSI/TechAmerica continuous maintenance program. Changes may be submitted at any time on any part of the standard using the TechAmerica Document Improvement Proposal at the back of this document or a similar method containing the same information. These comments shall be acted on for revision of the standard at the first meeting following working group resolution of the comment.

Published by

© 2008 TechAmerica
Standards & Technology Department
601 Pennsylvania Ave., NW
North Building, Suite 600
Washington, DC 20004-2650

PLEASE!

DON'T VIOLATE
THE
LAW!

TechAmerica

Standard Best Practices for System Safety Program Development and Execution

GEIA-STD-0010

Revision	Description of change	Date
-	Initial Release	Oct 2008

Contents

Figures

Tables

Foreword

This standard describes the best practices for applying system safety, the discipline of identifying and mitigating mishap risk encountered in the development, test, production, use, and disposal of systems, subsystems, equipment, and facilities. Risks are identified, evaluated, and mitigated to levels as low as reasonably practicable. Levels of risk must also be compliant with federal laws and regulations, executive orders, treaties, and agreements. Program trade studies associated with mitigating mishap risks must consider total life cycle cost in any decisions. Mishap risks associated with an individual system must be reported to and accepted by the Managing authority. When this standard is required in a solicitation or contract and no specific references are included, then only those requirements presented in Section 4 are applicable.

Early identification and control of safety critical hardware, software, human systems integration, and operations is the key to achieving a successful system safety program. Functional hazard analysis and assessment has historically been the most effective technique to determine hazards and develop safety requirements to mitigate risks. Coupled with use of the system safety risk mitigation order of precedence, functional hazard analysis lets a program identify early in the life cycle those risks which can be eliminated by design, and those which must undergo mitigation by other controls in order to reduce risk to an acceptable level. Finally, verification through documented evidence of compliance with safety requirements and safety features is necessary.

The G-48 System Safety Committee of the Information Technology Association of America, or ITAA (formerly GEIA), developed this document.

Background

This document outlines standard best practices for the setup, implementation, and management of system safety programs. System safety is an engineering discipline that can be applied to any activity to reduce or manage the risk of harm to people, property, or the environment. The formalization of system safety as a distinct discipline can be traced back at least as far as the 1940s. The 1960s saw the development and publishing of the first widely used standards for the practice of System Safety, including MIL-STD-882 in 1969, which evolved from some earlier U.S. military and Air Force specifications.

Over the next 30 years, several revisions to MIL-STD-882 were published, the most recent being Revision D in 2000. The ITAA (formerly GEIA) G-48 System Safety Committee played a key role in the development and publishing of every revision of MIL-STD-882. In response to Acquisition Reform initiatives of the mid-1990s, many military standards were cancelled or threatened with cancellation. To spare MIL-STD-882 from cancellation, the G-48 Committee prepared and submitted Revision D as a less prescriptive version, with the system safety tasks, data item descriptions (DIDs), and a great deal of other specific guidance and standard practices from Revision C and earlier revisions removed.

By the mid-2000s, the G-48 Committee saw, in general, a need to prepare a major new revision of MIL-STD-882 that would restore the specificity removed for the D Revision, and that would incorporate several other improvements. These improvements included:

(1) adjusting the organizational arrangement of information to clarify the basic elements of a system safety program and the process flow among them,

(2) modernizing the document and its tools—such as the Risk Assessment Matrix—to bring them abreast of contemporary best practice, and

(3) introducing—though not requiring—the concept of risk summation.

A G-48 working group prepared a draft Revision E of MIL-STD-882 to incorporate these improvements. This Draft MIL-STD-882E was prepared between August 2004 and February 2006 and regularly reviewed by the full G-48 Committee over the course of several G-48 Committee meetings. All review comments received during this process were thoroughly tracked, adjudicated, and incorporated as necessary. The resulting 1 February 2006 version of the G-48 Committee's Draft MIL-STD-882E was formally coordinated through and approved by nearly all the designated DoD standardization officials. A key non-concurrence from the DoD Acquisition Environment, Safety, and Occupational Health (ESOH) Integrated Product Team (IPT) resulted in control of the document being transferred to the ESOH IPT for a rewrite.

Amid concerns that the ESOH IPT's rewrite would eliminate many of the extensive improvements of its Draft Revision E, the G-48 Committee embarked on a parallel path to prepare a non-military system safety standard that would be published independently of MIL-STD-882, and that would include the modernization and improvements of the Draft Revision E. The approach followed was to start with the 1 February 2006 version of the G-48 Draft MIL-STD-882E, revise the text where necessary to remove all DoD-specific and military-specific language, and submit for publishing as a GEIA standard. The document submitted herewith is the result of this effort and has been designated GEIA-STD-0010, "Standard Best Practices for System Safety Program Development and Execution."

1 Scope

This document outlines a standard practice for conducting system safety. The system safety practice as defined herein provides a consistent means of evaluating identified risks. Mishap risk must be identified, evaluated, and mitigated to a level as low as reasonably practicable. The mishap risk must be accepted by the appropriate authority and comply with federal (and state, where applicable) laws and regulations, executive orders, treaties, and agreements. Program trade studies associated with mitigating mishap risk must consider total life cycle cost in any decision.

This document is intended for use as one of the elements of project solicitation for complex systems requiring a systematic evaluation of safety hazards and mitigating measures. The Managing authority may identify, in the solicitation and system specification, specific system safety engineering requirements to be met by the Developer. These may include risk assessment and acceptance criteria, unique classifications and certifications, or mishap reduction needs unique to their program. Additional information in meeting program specific requirements is located in the Appendixes.

2 Reference Documents

Information on safety analysis techniques is available from the documents listed below.

Nothing in this section or the documents listed below supersedes applicable laws and regulations unless a specific exemption has been obtained.

- ***System Safety Analysis Handbook***. System Safety Society, P.O. Box 70, Unionville, VA 22567.
- ***System Safety Design Handbook***, DH 1-6, Aeronautical Systems Center, Wright-Patterson Air Force base OH.
- ***Advisory Circular (AC) No. 25.1309-1A*** – "System Design and Analysis." Washington D.C., FAA.
- ***Aerospace Recommended Practice 4761*** *(ARP4761), Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.* Society of Automotive Engineers, Warrendale, PA.
- ***IEEE Standard for Software Safety Plans***, IEEE **Standard** 1228.

3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Acronyms Used in this Standard.

The acronyms used in this standard are defined as follows:

AC	Advisory Circular
AE	Architect and Engineering Firm
ALARP	As Low as Reasonably Practicable
ANSI	American National Standards Institute
ARP	Aerospace Recommended Practice
CDRL	Contract Data Requirements List

COTS	Commercial Off The Shelf
CSCI	Computer Software Configuration Item
CSI	Critical Safety Item
ECP	Engineering Change Proposal
ENG	Engineering
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
ESF	Engineered Safety Feature
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FTA	Fault Tree Analysis
G-48	System Safety Committee of GEIA
GEIA	Government Electronics and Information Technology Association
GOTS	Government Off The Shelf
HF	Human Factors
HHA	Health Hazard Assessment
HSI	Human Systems Integration
HTS	Hazard Tracking System
IMS	Integrated Master Schedule
IPT	Integrated Product Team
IRS	Interface Requirements Specification
ISSPP	Integrated System Safety Program Plan
ITAA	Information Technology Association of America
IV&V	Independent Verification and Validation
MA	Managing authority
MGT	Management
MRAL	Mishap Risk Acceptance Level
N/A	Not Applicable
NEPA	National Environmental Policy Act
NSC	Not Safety Critical
O&SHA	Operating and Support Hazard Analysis
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager

PSSA	Preliminary System Safety Assessment
PTR	Program Trouble Report
QRA	Quantitative Risk Assessment
SAE	Society of Automotive Engineers
SAR	Safety Assessment Report
SCC	Software Control Category
SCCSC	Safety Critical Computer Software Component
SCF	Safety Critical Function
SCI	Software Criticality Index, Safety Critical Item
SCN	Specification Change Notice
SDP	Software Development Plan
SDR	System Design Review
SHA	System Hazard Analysis
SIAM	Software Integrity Assurance Matrix
SOW	Statement of Work
SPR	Software Problem Report
SQA	Software Quality Assurance
SRCA	Safety Requirements/Criteria Analysis
SRR	System Requirements Review
SRS	Software Requirements Specification
SSA	System Safety Assessment
SSI	Safety Significant Item
SSG	System Safety Group
SSHA	Subsystem Hazard Analysis
SSMP	System Safety Management Plan
SSPP	System Safety Program Plan
SSR	Software Specification Review
SSS	System/Segment Specification
SSWG	System Safety Working Group
STP	Software Test Plan
WBS	Work Breakdown Structure

3.2 Definitions

Definitions used in this standard may differ from those used in other standards. In interpreting and applying this standard, care must be taken to ensure that use of these terms is consistent with their definitions as found herein. Within this document, the following definitions apply:

Acquisition program

A directed, funded effort designed to provide a new, improved, or continuing system in response to a validated operational need.

As low as reasonably practicable (ALARP)

That level of risk which can be further lowered only by an increment in resource expenditure that cannot be justified by the resulting decrement in risk. Often identified or verified by formal or subjective application of cost-benefit analysis or multi-attribute utility theory.

Acceptable Risk

That level of residual safety risk that the managing authority is willing to assume on behalf of the agency, users, and public.

Asset.

Something of value. Assets include but are not limited to personnel, facilities, equipment, operations, data, the public, and the environment, as well as the system itself.

Critical characteristic.

Any feature throughout the life cycle of a Critical Safety Item, such as dimension, tolerance, finish, material or assembly, manufacturing or inspection process, operation, field maintenance, or depot overhaul requirement that if non-conforming, missing, degraded or absent could result in a mishap with consequences unacceptable to the Managing authority.

Critical Safety Item.

A part, subassembly, assembly, subsystem, installation equipment, or support equipment for a system that contains a characteristic, any failure, malfunction, or absence of which could result in an mishap as defined by the Managing authority.

De minimis threshold.

The level of mishap risk below which a hazard does not warrant any expenditure of resources to track or mitigate. From the Latin phrase "*de minimis non curat lex"* which means "the law does not concern itself with trifles."

Design control activity.

The entity (person, organization, or function) that is specifically responsible for ensuring that all system requirements, including safety, are designed into a system or equipment.

Developer.

The individual or organization assigned responsibility for a development effort.

Development agreement.

Formal documentation of the agreed-upon tasks that the Developer must execute for the program. For a commercial Developer, this agreement usually is in the form of a written contract.

Engineered Safety Feature (ESF).

An actively functioning design feature included in the system to reduce the mishap risk. ESFs generally involve a system element that is automatically actuated, though provisions for manual actuation may exist. Examples of ESFs include the emergency core cooling system of a nuclear reactor and loss-of-tension braking for elevators.

Fail Safe.

A system attribute involving incorporation of a feature to automatically counteract the effect of an anticipated possible source of failure, although at the otherwise harmless sacrifice of functions.

Functional hazard assessment (FHA).

A systematic, comprehensive top-down examination of functions to identify and classify failure conditions of those functions according to their severity and assigning, to each failure condition probability, requirements and applicable qualitative design requirements.

Hazard

(1) Potential for harm

(2) a condition prerequisite to a mishap."

Mishap description

A hazard description contains the means by which the source can bring about the harm.

Hazardous

Containing some element of safety risk and capable of inflicting harm.

Hazardous Function

A function that, if performed inadvertently, performed incorrectly, performed out-of-sequence, or not performed, could result in a mishap unacceptable to the managing authority.

Hazardous material

Any substance that, due to its chemical, physical, or biological nature, causes safety concerns that would require an elevated level of effort to manage.

Health hazard assessment (HHA)

The application of biomedical knowledge and principles to identify and eliminate or mitigate health hazards associated with systems in direct support of the life cycle management of materiel items.

Human Factors

A disciplined, unified, and interactive approach used to integrate human considerations into system design, improve total system performance, and reduce costs of ownership. The major considerations of Human Factors include: human factors ergonomics, manpower and personnel, training, and occupational safety and health.

Life cycle

All phases of the system’s life including concept refinement, technical development, system development and demonstration, production and deployment, operations and support, and disposal.

Managing authority

The entity that has management responsibility for the system, or Developer who imposes system safety tasks on their suppliers.

Mishap (accident)

An unplanned event or series of events resulting in death, injury, system damage, or loss of or damage to equipment or property.

Mishap description.

A brief narrative description of a potential mishap attributable to the hazard. A mishap description contains three elements: the source, an activity or a condition that serves as the root; the mechanism, a means by which the source can bring about the harm; and an outcome, the harm itself that might be suffered.

Mishap frequency

Rate of mishap occurrence. Frequency is sometimes substituted for probability as a component of risk (example: loss events per 10^6 operating hours).

Mishap Likelihood

Likelihood of mishap occurrence over a specified exposure interval. Probability is expressed as a value between zero and one. Probability is a component of risk and has no dimension but must be attached to an interval of exposure (example: one operating year, a million vehicle miles).

Mishap probability category

A component of the mishap risk assessment matrix. A categorization that provides a range of probabilities (or likelihoods) for the occurrence of a mishap.

Mishap risk assessment

The process of characterizing hazards within risk areas and critical technical processes, analyzing them for their potential mishap severity and probability (or likelihood) of occurrence, and prioritizing them for risk mitigation actions.

Mishap risk category

A specified range of risk associated with a given level (high, serious, medium, low) used to prompt specific action such as reporting hazards to appropriate management levels for risk acceptance.

Mishap severity

An assessment of the potential degree of harm from a mishap. Severity is one component of risk.

Mishap severity category

A component of the mishap risk assessment matrix. A categorization that delineates a range of mishap outcomes in terms of fatalities, injuries, property damage, or other loss.

Mitigator

A feature of a system that reduces risk for one or more hazards by lowering either the probability of a harmful outcome or the severity of such an outcome, should it occur. Also referred to as a control, a hazard control, a control measure, a countermeasure, a mitigating measure or a mitigation.

Program manager

An official who is responsible for managing a development program. Also, a general term of reference to those organizations directed by individual managers, exercising authority over the planning, direction, and control of tasks and associated functions essential for support of designated systems. This term will normally be used in lieu of any other titles, e.g.; system support manager, system manager, and project manager.

Risk (also referred to as mishap risk)

A measure of the expected loss from a given hazard or group of hazards. Risk is a combined expression of loss severity and probability (or likelihood). When expressed quantitatively, risk is the simple numerical product of severity of loss and the probability that loss will occur at that severity level. This term has the following applications:

Single hazard risk (r)

Risk associated with a single hazard of the system. A single hazard risk is typically characterized by a severity-probability pair, assessed using a mishap risk assessment matrix.

Total Mishap risk (R)

An expression of overall system risk, comprising the combined separate properties of all partial risks.

Residual mishap risk

The mishap risk that remains after all approved mitigators have been implemented and verified. (Interim risk is the risk that is present until final mitigation actions have been completed.)

Risk driver

A characteristic that meaningfully contributes to the severity and/or the probability of the risk posed by one or more system hazards

Safety

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

Safety critical

A term applying to those items, units, components, subsystems, or systems whose failure and/or hazard may result in major system damage, death, severe injury, or could result in a mishap with consequences unacceptable to the Managing Authority.

Safety critical function

A function that, if not performed, could result in mishap as defined by the applicable managing authority.

Safety device

In general, these are static interveners included in the system to reduce mishap risk. Examples include physical guards, revetments, guardrails, toeboards, machine guards, safety eyewear, hearing protection, and barricades. Safety devices installed onto or as part of the system, such as physical guards or barricades, should be distinguished from those

requiring personal use, such as safety eyewear, hearing protection, or other items of personal protective equipment because they are less dependent on user intervention.

Safety significant item (SSI)

A function, subsystem, or component, the failure of which (including degraded functioning or functioning out of time or out of sequence) could result in a significant mishap as defined by the Managing authority.

Software control category (SCC)

The level of control a particular software function has over the identified hazard.

Software criticality index (SCI)

A measure of the degree of importance that the software will perform a specific function correctly to achieve mishap risk as low as reasonably practicable in the operation of the system.

Subsystem

A grouping of items satisfying a logical group of functions within a particular system.

System

(1) An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective. A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, and software.

(2) The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.

System engineering

A comprehensive, iterative technical management process that includes translating operational requirements into configured systems, integrating the technical inputs of the entire design team, managing interfaces, characterizing and managing technical risk, transitioning technology from the technology base into program specific efforts, and verifying that designs meet operational needs. It is a life cycle activity that demands a concurrent approach to both product and process development.

System safety

The application of engineering and management principles, criteria, and techniques to achieve mishap risk as low as reasonably practicable (to an acceptable level), within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

System safety engineering

An engineering discipline that employs specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and mitigate hazards, in order to reduce the associated mishap risk.

System safety management

All plans and actions taken to identify, assess, mitigate, and continuously track, control, and document mishap risks encountered in the concept, development, test, acquisition, use, and disposal of systems, subsystems, equipment, and facilities.

System safety management plan (SSMP)

A management plan that defines the system safety program requirements. The SSMP ensures the planning, implementation, and accomplishment of system safety tasks and activities consistent with the overall program requirements.

System safety program plan (SSPP)

A formal document that fully describes the planned safety tasks required to meet the contractual systems safety requirements including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems. It may also define the minimum level of safety required by the program and the approaches for addressing the safety of complex integrated systems.

Technical data package

A technical description of an item that is adequate to support an acquisition strategy, production, engineering, and logistics. The description defines the required design configuration and procedures required to ensure adequacy of item performance. It consists of all applicable technical data such as drawings or automated models and associated lists, specifications, standards, performance standards, quality assurance requirements, software and packaging details.

White Box Testing

Testing software with the knowledge of the internal structure and coding inside the program.

4 General Requirements

This section delineates the minimum mandatory requirements for an acceptable system safety program for any system. The PM must establish and maintain a system safety program to achieve the overall system safety objectives for the program. This section prescribes the system safety program elements to be performed throughout the life cycle for any system. These guidelines are to ensure the identification and understanding of mishap hazards and their associated risks. The objective of system safety is to reduce mishap risk to an acceptable level (or alternatively as low as reasonably practical) through a systematic approach of hazard analysis, risk assessment, and risk management.

4.1 System Safety Program Elements.

The Managing authority must establish and execute system safety programs that manage the risk of each single hazard (r) as well as the total system (R). The following five elements are necessary to conduct a complete system safety program. Within each of the elements, the managing authority and developer must tailor the system safety program to fit the system context, unique hazards, and fiscal limitations. The Managing authority must allocate sufficient resources to accomplish each safety element. Additional guidance on system safety program tailoring can be found in Section A.3.1.2.1.

4.1.1 Element 1 — Program Initiation

The Managing authority must document the approved system safety engineering approach and other actions needed to establish a fully functional system safety program. Guidance can be found in Section A.3.1.

4.1.2 Element 2 — Hazard Identification and Tracking

System safety includes a complete identification of the hazards associated with a system. In general this is accomplished by identifying the source-mechanism-outcome of each hazard. This element also includes use of a hazard tracking system (HTS) and continuous tracking of the hazards throughout the life cycle. Guidance can be found in Section A.3.2.

4.1.3 Element 3 — Risk Assessment

For each identified hazard, the mishap severity and probability or frequency are established. A mishap risk assessment matrix (Section A.5) is used to assess and display the risks. The assessment methods may include models, numerical analyses, and subjective judgments based on history and system knowledge. Guidance can be found in Section A.3.3.

4.1.4 Element 4 — Risk Reduction

Risk reduction is achieved by accomplishing the following steps.

a. Understand the risk drivers.
b. Develop and document candidate mitigators.
c. Select and implement mitigators in accordance with the system safety mitigation order of precedence.
d. Verify that the risk has been reduced.

Implementation details are described in Section A.3.4.

4.1.4.1 System Safety Mitigation Order of Precedence

In reducing risk, the cost, feasibility, and effectiveness of candidate mitigation methods must be considered. In evaluating mitigation effectiveness, an order of precedence generally applies as follows.

4.1.4.1.1 Eliminate Hazard Through Design Selection

Ideally, the risk of a hazard will be eliminated. This is often done by selecting a design alternative that removes the hazard altogether. Examples include: choosing pneumatic controls rather than electrical controls for application in an explosive atmosphere; preventing entrapment by equipping refrigerator doors with magnetic strip gaskets rather than using positive latching hardware door closures; selecting a non-flammable hydraulic fluid rather than a flammable one; replacement of toxic materials with benign materials.

4.1.4.1.2 Reduce Mishap Risk Through Design Alteration.

If the risk of a hazard cannot be eliminated by adopting an alternative design, design changes must be considered that reduce the severity and/or the probability of a harmful outcome. Examples include: minimizing the quantity of a hazardous intermediate agent in a chemical process; placing a current-limiting resistor in the discharge circuit of a high energy electrical circuit; providing flow-tripping flutes on discharge stacks to prevent resonant vortex shedding. Examples of safety design requirements used to reduce risk appear in Section A.6.

4.1.4.1.3 Incorporate Engineered Safety Features (ESF)

If unable to eliminate or adequately mitigate the risk of a hazard through a design alteration, reduce the risk using an ESF that actively interrupts the mishap sequence. Examples include: the emergency core cooling system of a nuclear reactor; loss-of-tension braking for elevators; full-time, on-line redundant paths; interlocks; ground-fault circuit interrupters; uninterruptible power supplies.

4.1.4.1.4 Incorporate Safety Devices

If unable to eliminate or adequately mitigate the hazard through design or ESFs, reduce mishap risk by using protective safety features or devices. In general, safety devices are static interveners. Examples include: physical barriers; machine guards; barricades; safety eyewear; hearing protectors. Safety devices installed onto or as part of the system, such as physical guards or barricades, should be distinguished from those requiring personal use, such as safety eyewear, hearing protection, or other items of personal protective equipment. Use of installed controls is generally preferable and more consistent with the system safety order of precedence. Additionally, the training component of protective equipment use needs to be considered as a procedure and training element that requires more ongoing resource commitment and is subject to more variables than safety devices intrinsic to the system.

4.1.4.1.5 Provide Warning Devices

If design selection, ESFs, or safety devices do not adequately mitigate the risk of a hazard, include a detection and warning system to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.

4.1.4.1.6 Develop Procedures and Training

Where other risk reduction methods cannot adequately mitigate the risk from a hazard, incorporate special procedures and training. Procedures may prescribe the use of personal protective equipment. For hazards that could result in mishaps as defined by the Managing authority, avoid using warning, caution, or written advisories or signage as the only risk reduction method.

4.1.5 Element 5 — Risk Acceptance

The Developer PM must provide the Managing authority with sufficient information to make informed decisions regarding the acceptability of residual mishap risk and the costs of risk mitigating measures. Risk communication must consider the risk of the individual hazard in context of the total system risk.

4.2 Normative Information

This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.

4.2.1 Intended Use

This standard establishes a common basis for expectations of a properly executed system safety effort.

4.2.2 Data Requirements

Hazard analysis data may be obtained from various sources. The managing authority is encouraged to request any type of safety plan required to be provided by the Developer in the proposal.

4.2.3 Subject Term (Key Word) Listing

- As low as reasonably practicable (ALARP)
- Environmental
- Hazard
- Mishap
- Mishap probability category
- Mishap risk category
- Mishap severity category
- Mitigator
- Risk
- System safety engineering
- System safety management
- Total system risk

4.2.4 Use of System Safety Data in Certification and Other Specialized Safety Approvals

Hazard analyses are often required for many related certifications and specialized reviews. Examples of activities requiring data generated during a system safety effort include:

- Federal Aviation Administration (FAA) airworthiness certification of designs and modifications.
- Airworthiness determination.
- Munitions certification.
- Flight readiness reviews.
- Flight test safety review board reviews.
- Test readiness reviews.
- Safety review boards for research, development, test, and evaluation.
- Nuclear Regulatory Commission licensing.
- Department of Energy certification.
- Third party (e.g., factory mutual, underwriters laboratories) subcomponent certification for specific items for support equipment type risk.

5 Detailed Requirements

The Managing authority must identify, in the solicitation and system specification, any specific system safety engineering requirements including risk assessment and acceptance, unique classifications and certifications, or any mishap reduction needs unique to their program. Additional information for use in developing program-specific requirements appears in Appendices A and B.

Appendix A — Guidance For Implementation of a System Safety Effort

A.1 Scope

This appendix provides rationale and guidance to fit the needs of most system safety efforts. It includes further explanation of the effort and activities available to meet the general requirements described in Section 4 of this Standard. With the exception of the paragraphs listed in Section 4, this appendix is not a mandatory part of this guide and is not to be included in solicitations by reference. However, portions of this appendix may be extracted for inclusion in requirement documents and solicitations.

A.2 Terms and Definitions

A.2.1 Acronyms used in this appendix

No additional acronyms are used in this appendix (see Section 3.1).

A.2.2 Definitions

No additional definitions are used in this appendix (see Section 3.2).

A.3 General Requirements

System safety applies engineering and management principles, criteria, and techniques to achieve ALARP (acceptable risk) within the constraints of operational effectiveness, time, and cost, throughout all phases of the system life cycle. It draws upon professional knowledge and specialized skills in the mathematical, physical, and scientific disciplines, together with the principles and methods of engineering design and analysis, to specify and evaluate the mishap risk to people, systems, and the environment associated with a system. Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given and the proper allocation of specific planning, requirements, analysis, testing, and verification tasks.

System safety program requirements can be grouped into the five major elements (Figure A-1):

Element 1—Program Initiation,

Element 2—Hazard Identification,

Element 3—Risk Assessment,

Element 4—Risk Reduction, and

Element 5—Risk Acceptance

Elements 1 and 5 are primarily system safety management-related functions and Elements 2, 3, and 4 are considered system safety engineering functions.

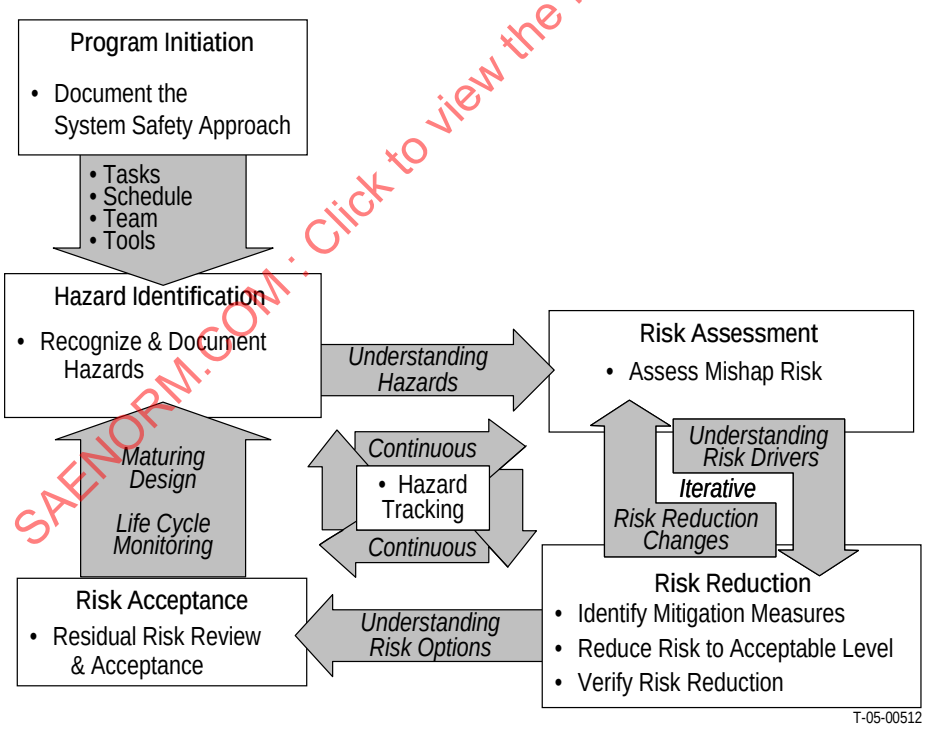


Figure A-1 — Safety Program Elements

A.3.1 Element 1 — Program Initiation

Program initiation is the foundation of the safety program. As shown in Figure A-2, it is important to establish the key elements and actions of the safety program in this element.

Products of Element 1 may include an SSMP, if required, an SSPP, and a charter for the System Safety Working Group (SSWG).

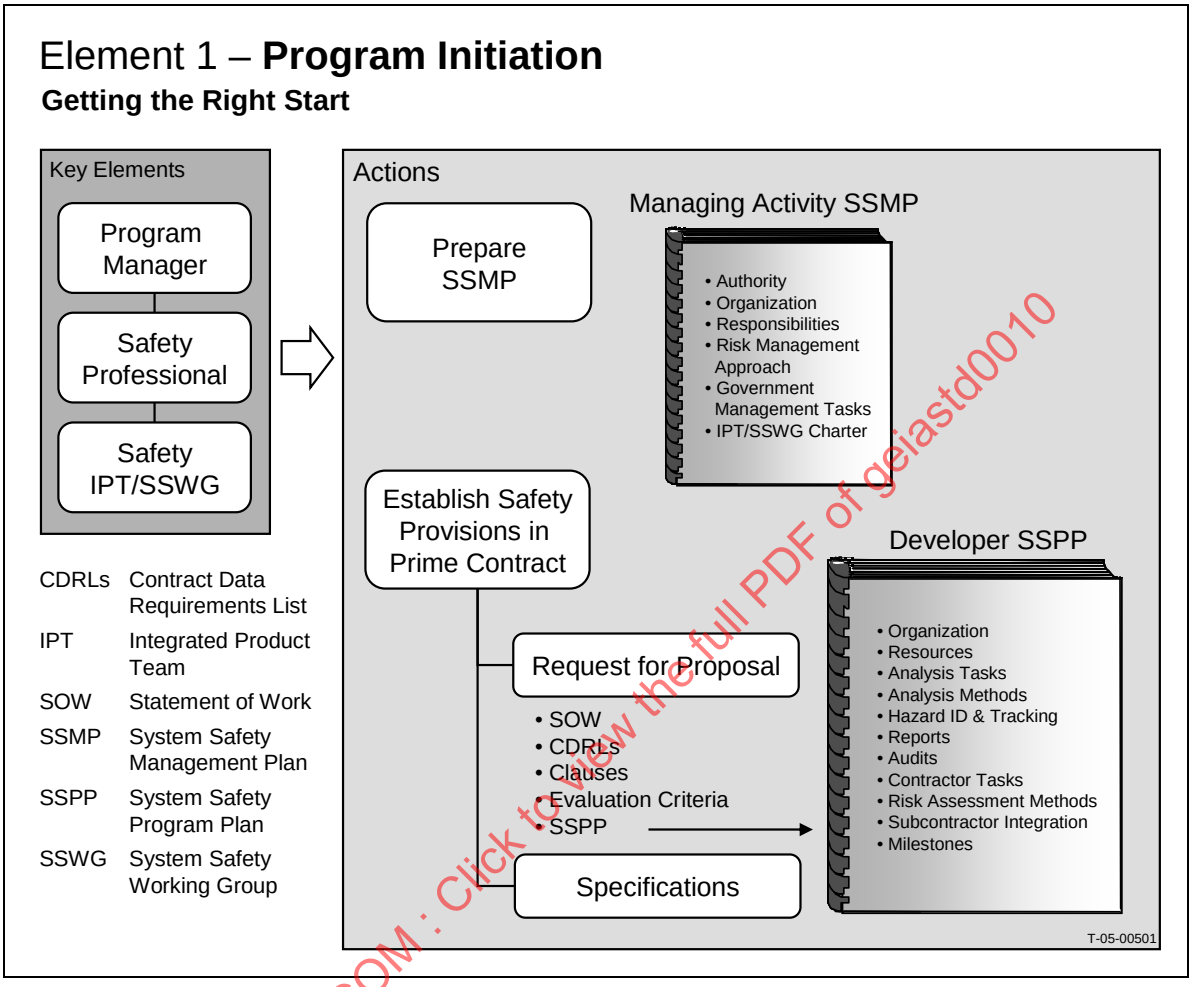


Figure A-2 — Program Element 1—Program Initiation

A.3.1.1 Define Program Authorizations and Charters

The Managing authority(ies) must establish and execute system safety programs that manage the risk of each single hazard (r) as well as the total system risk (R). Provisions for system safety requirements and effort as defined by this standard must be included in all applicable contracts. Properly initiated programs must be formalized in documentation approved by the Managing authority indicating the actions to be taken by the safety organization.

A.3.1.2 Plan a System Safety Program

Before formally documenting the system safety approach in the SSMP and contract statement of work (SOW), the Developer, in concert with system safety professionals, must determine what system safety effort and specific tasks and activities are necessary to meet program and regulatory requirements. This requires the system boundaries and usage context to be clearly defined within the plan, including assumptions that establish the depth and breadth of the analyses. This effort includes developing a planned approach for safety task accomplishment,

providing qualified people to accomplish the tasks, establishing the authority for implementing the safety tasks through all levels of management, and allocating appropriate resources to ensure that the safety tasks are completed. This is an on-going process to include additional analysis based on findings from previous efforts. System safety planning includes the following.

A.3.1.2.1 Tailor the Program

Selective tailoring of a system safety program is necessary to effectively achieve all of the safety objectives within the constraints of performance, cost, schedule, and potential mishap loss. As such, tailoring becomes an important aspect of establishing an effective and successful program. Some of the important aspects to consider include the following.

A.3.1.2.1.1 Tasks

Individual tasks from Appendix B will be applied as needed for a particular program. A large and/or complex safety critical system will likely require more tasks than a smaller system.

A.3.1.2.1.2 Analyses

Specify only those safety analyses necessary for the particular program. For example, a safety critical system (aircraft, missile, air traffic control, ships, mass transit, etc.) may need a preliminary hazard list (PHL), preliminary hazard analysis (PHA), functional hazard assessment (FHA), preliminary system safety assessment (PSSA), system safety assessment (SSA), subsystem hazard analyses (SSHA), system hazard analysis (SHA), operating and support hazard analysis (O&SHA), safety assessment report (SAR), health hazard assessment (HHA), safety requirements/criteria analysis (SRCA), and Critical Safety Item (CSI) List. A less-safety-critical system may only need a PHL and PHA for an effective system safety program.

A.3.1.2.1.3 Mishap Risk Assessment Matrix and Scaling

The method of risk assessment and representation used by the program will be selected and tailored to fit practical program needs. For some programs, a quantitative risk assessment matrix may be appropriate, while others may require a qualitative (subjective) matrix. Matrix axis scaling will also be tailored to match practical program needs. For example, systems for which loss events carry very small penalties will require correspondingly lower matrix severity scale values than those capable of producing very costly losses. Similarly, matrices for systems capable of high cost losses will customarily require probability scaling at lower values than those for systems having only low cost loss expectancy.

A.3.1.2.1.4 Acceptance Levels

The risk acceptance levels that are appropriate to the particular product or system. Different size and complexity programs may utilize different levels.

A.3.1.2.1.5 Preferred Formats

Determine the preferred format of the safety and hazard analyses. For example, the SSPP for a system of systems type program may desire to standardize the analyses formats for all of the lower tier systems and elements involved.

A.3.1.2.1.6 Verification Methods

Determine the safety verification methods to be utilized. Depending upon the program size and level of risk, some programs may require more testing while others may need less testing and more analysis.

A.3.1.2.1.7 System Safety Program Plan (SSPP)

The SSPP must describe and document the tailored system safety program. The SSPP must contain a description of the planned methods to be used to implement the tailored requirements of this standard, including organizational responsibilities, resources, methods of accomplishment, milestones, analyses, depth of effort, risk characterization and integration with other program engineering and management activities and related systems.

A.3.1.2.2 Establish Safety Performance Requirements

Establish specific safety performance requirements based on overall program requirements and system user inputs. These are the general safety requirements needed to meet the core program objectives. The more closely these requirements relate to a given program, the more easily the designers can incorporate them into the system. It may be helpful to start with requirements from a similar system. In the appropriate system specifications, incorporate the safety performance requirements that are applicable, and the specific risk levels considered acceptable for the system. Acceptable risk levels can be defined in terms of a mishap risk category developed through a mishap risk assessment matrix; an overall system mishap rate; demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards and regulatory requirements; or other suitable mishap risk assessment procedures. Examples of safety performance statements are in the following subparagraphs.

A.3.1.2.2.1 Quantitative Requirements

Quantitative requirements may be expressed in terms of either risk, or the probability or frequency of a given mishap severity category. Risk measures are typically expressed as a loss rate, such as: “The expected dollar loss per flight hour must not exceed $XXXX” or “The expected fatalities per year must not exceed 0.00X.”

A.3.1.2.2.2 Mishap Risk Requirements

Mishap risk requirements could be expressed as “no hazards assigned a catastrophic mishap severity as defined by the System Safety Management Plan are acceptable.” Mishap risk requirements could also be expressed as a level defined by a mishap risk assessment, such as “no serious mishap risks or higher are acceptable.”

A.3.1.2.2.3 Standardization Requirements

Standardization requirements are expressed relative to a known standard that is relevant to the system being developed. Examples include: “The system must comply with the laws of the State of Xxxxxxxx and be operable on the highways of the State of Xxxxxxxx” or “The system must be designed to meet American National Standards Institute (ANSI) STD XXXX.XX-XXXX as a minimum.”

A.3.1.2.3 Establish a System Safety Organization

Establish a system safety organization or function and the required lines of communication with associated organizations. Establish interfaces between system safety and other functional elements of the program, as well as with other safety related disciplines (such as nuclear, range, occupational health, explosive, chemical, and biological). Designate the organizational unit responsible for executing each safety task. Establish the authority for resolution of identified hazards. Define resources needed, to include the SSWG and if necessary integrated product teams (IPTs). Organizational interface and an integrated master schedule (IMS) must be included.

A.3.1.2.4 Establish System Safety Milestones

Establish system safety milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs.

A.3.1.2.5 Establish an Incident Alerting/Notification, Investigation, and Reporting Process

Establish an incident alerting/notification, investigation, and reporting process, to include notification of the Managing authority and Developer.

A.3.1.2.6 Establish Acceptable Levels

Establish an acceptable level of mishap risk, mishap probability or frequency, and mishap severity thresholds, and documentation requirements (including but not limited to hazards and mishap risk).

A.3.1.2.7 Establish a Reporting Approach and Methodology

Establish an approach and methodology for reporting to the Managing authority the following minimum information:

- Safety critical characteristics and features.
- Critical Safety Items.
- Operating, maintenance, and overhaul safety requirements.
- Measures used to eliminate or mitigate hazards.
- Selection, acquisition, and process management for hazardous materials.

A.3.1.2.8 Establish the Method for Formal Acceptance and Documentation

Establish the method for the formal acceptance and documentation of mishap risks and the associated hazards.

A.3.1.2.9 Establish the Communication Method

Establish the method for hazards, the associated risks, and mishap risk to the system user.

A.3.1.2.10 Specify Requirements for Other Specialized Safety Approvals

Specify requirements for other specialized safety approvals (e.g., nuclear, explosive, chemical, biological, electromagnetic radiation, and lasers) as necessary (reference Sections 4.2.4).

A.3.1.2.11 Specify the Typical Boundaries and Assumptions

Specify the typical boundaries and assumptions for the system safety analyses and the typical limits of the analyses. These may include whether or not the following are examined and/or analyzed:

- Hostile intentions or sabotage upon the system.
- Basic structural integrity.
- Hazards unique to factory support.
- The assumption that only trained, healthy, working-age adults will operate and support the system.
- Appropriate quality control and configuration standards are used in production, assembly and support.

A.3.1.2.12 Establish the Plan for Updating the Hazard analyses

Hazard analyses have limited resolution depending on the system and details of the hazards. Analyses will be updated as more information is acquired.

A.3.1.3 Develop a System Safety Management Plan.

This plan documents the Developer's approved system safety engineering and management approach. It must include the information called out in the following subparagraphs.

A.3.1.3.1 Overall System Safety Integration

Information on system safety integration into the overall program structure.

A.3.1.3.2 Software System Safety Integration

Where software controls or mitigates system hazards, include specific details on integration of system safety processes and products into the software development life cycle. As a minimum address the following topics:

a. Identification and description of software contributors to hazards;
b. Definition of safety critical;
c. Identification of safety critical software functions and safety critical software requirements;
d. Identification of the software hazard criticality assessment process to include establishment of the software criticality index matrix (see Section A.6) for each safety critical software function and safety critical requirement and how it will be used to assign software integrity assurance tasks necessary to verify and validate the safety critical functions and requirements;
e. Performing a final risk assessment for hazards which have software contributors.

A.3.1.3.3 Hazard Closure and Risk Acceptance Process

Define how hazards and mishap risks are communicated to and accepted by the appropriate risk acceptance authority and how hazards and mishap risk will be tracked.

.3.1.3.4 The Mishap Risk Assessment Tool

Define the mishap risk assessment tool used for risk assessment and acceptance. A key part of the approach for system risk management is the adoption of an appropriate mishap risk assessment matrix. Mishap risk assessment matrices provide a means to assess and communicate risks and establish authority for acceptance of those risks. Programs may use one matrix to assess risks from individual hazards, and another matrix to accept total system risk. These tools must be defined during the planning phase; however, they may need tailoring or refinement during Element 2 as the full set of hazards becomes more apparent. A software hazard criticality assessment and software safety integrity assessment must be performed for each safety critical software function and associated safety critical requirement (see Section A.6). Upon completion of all the software safety engineering analyses tasks and the software integrity assurance tasks a final risk assessment can be performed based on the confidence gained in the software (see Section A.6.3).

A.3.1.3.4.1 Use of the Mishap Risk Assessment Matrix

The mishap risk assessment matrix is normally a two-dimensional graphic device. One axis is scaled to represent mishap severity, and the other is scaled to represent mishap probability or frequency. The four principal uses of the matrix are:

a. Communicates the range of potential risks of the system in terms of mishap severity and mishap probability or frequency;
b. Guides assessment of risk for single hazards;
c. Displays the results of risk assessments, risk mitigation and reduction; and
d. Delineates risk acceptance decision authority.

A.3.1.3.4.2 Guidance in Developing Mishap Risk Assessment Matrices

All systems have unique risks. A mishap risk assessment matrix will be used to characterize these risks. A pre-existing matrix may be used or a uniquely tailored matrix may be developed. In developing and tailoring the risk matrix, these elements must be considered:

a. Tailor mishap risk assessment matrices to each system or class of systems based on the expected range of severity of potential mishaps and the range of probability or frequency of these mishaps.
b. Orient the severity and probability (or frequency) axes so that one axis increases upward and the other increases to the right in accordance with the Cartesian coordinate system.
c. Use logarithmic scales on each axis with logical and proportional ranges for mishap severity categories and mishap probability categories.
d. Assign the four levels of risk acceptance authority (high, serious, medium, low) to each cell of the matrix.

A.3.1.3.4.3 Mishap Risk Assessment Matrix Tailoring

New or tailored matrices must be developed by defining and scaling the severity and probability or frequency scales that bound the risk of the system. Examples of a tailoring approach and tailored matrices are provided in Section A.5.

A.3.1.3.4.4 *De Minimis* Threshold

In defining the mishap risk assessment matrix, programs may also wish to define a *de minimis* threshold. The term *de minimis* is short for the Latin *de minimis non curat lex* which means “the law does not concern itself with trifles.” This concept, adapted from the legal profession, helps define the action thresholds. Hazards below this threshold have risk so low that they do not warrant any additional expenditure of resources. Below this threshold, there is no requirement to actively track the hazard, though it may be mitigated if minimal resources are required. Hazards above the *de minimis* line are the focus of the system safety program. Generally, for hazards with greater risk, greater risk reduction resources are warranted. See Figures A-10, A-11, and A-12 for examples of a *de minimis* threshold.

A.3.1.3.4.5 Additional Safety Plan Requirements

- Describe how changes to design, training, and technical manuals for the purpose of risk mitigation will be accomplished.
- Describe the verification (e.g., test, analysis, demonstration, or inspection) requirements for ensuring that safety is adequately attained. Identify any certification requirements for

software, safety devices, or other special safety features (e.g., render safe and emergency disposal procedures).

- Describe the mishap or incident notification, investigation, and reporting process for the program, including notification of the Managing authority.
- Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned data. Include a description on how a system hazard log is developed and maintained.
- Describe how the user is kept informed of mishap risk and the associated hazards.
- Describe the approach to the identification, management, and control of Critical Safety Items.

A.3.1.4 Define a Strategy to Ensure Appropriate Safety Support

Elements of safety need to be embedded in the prime contractor's SOW and, if necessary, supporting contracts. Contractors will be required to submit with their proposal a preliminary plan (e.g., SSPP) that describes the system safety effort required for the requested program. When directed by the PM, attach this preliminary plan to the contract or reference it within the SOW; so it becomes the basis for a contractual system safety program.

A.3.1.4.1 Individual Safety Support Tasks

Include selected tasks from Appendix B. Individual tasks will be applied as needed for the particular program. Some programs may require only one or two tasks (e.g., a single PHA or a safety assessment report (SAR)), while other more complex programs may require application of most or all of the tasks. The documentation of the system safety approach must describe the planned tasks and activities of system safety management and systems engineering required to identify, evaluate, and eliminate or mitigate hazards. The goal of this effort is to reduce the mishap risk to a level ALARP throughout the system life cycle. The documentation must describe, as a minimum: a planned approach for task accomplishment, qualified people to accomplish tasks, the authority to implement tasks through all levels of management, and the appropriate commitment of resources (both manning and funding) to ensure that safety tasks are completed. Specifically, the documentation must:

A.3.1.4.1.1 Scope

Describe the scope of the overall system program and the related system safety effort.

A.3.1.4.1.2 Milestones

Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.

A.3.1.4.1.3 Safety Tasks and Activities

Describe the safety tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety and reference where they are specified or described. Include the organizational relationships between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization including the review and approval authority of those tasks.

A.3.1.4.1.4 Program-Specific Safety Tasks

Select tasks to fit the program. In most cases, the need for the tasks is self-evident. While experience plays a key role in task selection, it must be supplemented by a more detailed study of the program. Consideration must be given to the size and dollar value of the program and the expected level of risk involved. The selection of tasks must be applicable not only to the program phase, but also to the perceived risks involved in the design and the funds available to perform the system safety effort. Table A-1 provides examples of typically tailored system safety programs based on size or project risk. Once recommendations for task applications have been determined and more detailed requirements identified, tasks and requirements can be prioritized and a “rough order of magnitude” estimate must be made of the time and effort required to complete each task. This information will be of considerable value in selecting the tasks which can be accomplished within schedule and funding constraints.

Table A-1 — Application Matrix for System Program Development

Task	Title	Task Type	Program Phase 0	I	II	III	IV
101	System Safety Program	MGT	G	G	G	G	G
102	System Safety Program Plan (SSPP)	MGT	G	G	G	G	G
103	Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering (AE) Firms	MGT	S	S	S	S	S
104	System Safety Program Review /Audits	MGT	S	S	S	S	S
105	System Safety Group (SSG)/System Safety Working Group (SSWG) Support	MGT	G	G	G	G	G
106	Hazard Tracking and Risk Resolution	MGT	S	G	G	G	G
107	System Safety Progress Summary	MGT	S	G	G	G	G
108	Launch Safety Program Requirements	MGT	S	S	S	S	S
109	Test Hazard Analysis Safety (Ground or Airborne Systems)	MGT	S	S	S	S	S
201	Preliminary Hazard List (PHL)	ENG	G	S	S	S	N/A
202	Preliminary Hazard Analysis (PHA)	ENG	G	G	G	GC	GC
203	Safety Requirements/Criteria Analysis (SRCA)	ENG	G	S	S	S	GC
204	Subsystem Hazard Analysis (SSHA)	ENG	N/A	G	G	GC	GC
205	System Hazard Analysis (SHA)	ENG	N/A	G	G	GC	GC
206	Operating and Support Hazard Analysis (O&SHA)	ENG	S	G	G	GC	GC
207	Health Hazard Assessment (HHA)	ENG	G	G	G	GC	GC
208	Functional Hazard Analysis (FHA)	ENG	G	G	G	GC	GC
209	Critical Safety Items (CSI) List	ENG	S	G	G	G	G
301	Safety Assessment Report (SAR)	ENG	S	S	S	S	S
302	Test and Evaluation Safety	ENG	G	G	G	G	G
303	Safety Review of ECPs, Specification Change Notices (SCN), Software Problem Reports (SPR), Program Trouble Reports (PTR), and Requests for Deviations and Waivers	ENG	N/A	G	G	G	GC
401	Safety Verification	ENG	S	G	G	S	S
402	Safety Compliance Assessment	ENG	S	G	G	S	S

NOTES:
TASK TYPE
ENG - System Safety Engineering
MGT - System Safety Management

PROGRAM PHASE
O Concept refinement
I Technology development
II System development and demonstration
III Demonstration, production and deployment
IV Operations and support

APPLICABILITY CODES
S Selectively Applicable
G Generally Applicable
GC Generally Applicable to Design Change
N/A Not Applicable

A.3.1.4.1.5 Analysis Techniques and Formats

Describe specific analysis techniques and formats to be used in quantitative or qualitative assessments of hazards.

A.3.1.4.1.6 Management Decision Process

Describe the process through which management decisions will be made (for example, timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, and program deviations). Include a description of how mishap risk is formally accepted and this acceptance is documented.

A.3.1.4.1.7 Developer Support to Certification Boards

Identify special support from the Developer to support certification boards.

A.3.1.4.2 Mishap Risk Assessment Procedures

Describe the mishap risk assessment procedures, including the mishap severity categories, mishap probability categories, and the system safety mitigation order of precedence that must be followed to satisfy the safety requirements of the program. State any subjective or quantitative measures of safety to be used for the mishap risk assessment process including any associated

criteria. Include system safety definitions that modify, deviate from, or are in addition to those in this standard or generally accepted by the system safety community.

A.3.1.5 Preliminary Understanding of Hazards

Develop a preliminary understanding of hazards and a related description or identification.. Each type of system has generic hazards that can be recognized before the design details are developed. This understanding will lead to the generation of a PHL.

A.3.1.6 Attributes of an Effective System Safety Program

Attributes of an effective system safety program include the following:

- Management is always aware of the mishap risks associated with the system, and formally documents this awareness. Hazards associated with the system are identified, assessed, tracked, monitored, and the associated risks are either eliminated or mitigated to an acceptable level throughout the life cycle. Identify and archive those actions taken to eliminate or reduce mishap risk for tracking and lessons learned purposes.
- Historical hazard and mishap data, including lessons learned from other systems, are considered and used.
- Mishap risk resulting from harmful conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration) and human error in system operation and support is minimized. Design factors likely to contribute to human error are identified and mitigated.
- System users are kept abreast of the safety of the system and included in the safety decision process.

A.3.2 Element 2 — Hazard Identification

Identify and track hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended usage or application. Historical hazard and mishap data, including lessons learned from other systems, must be considered and used. Identification of hazards is a responsibility of all program members. During hazard identification and tracking; consider hazards that could occur over the system life cycle. Products of this element may include a PHL and/or a functional hazard assessment and a hazard tracking system (HTS). Figure A-3 describes the process, methods, and products of this element.

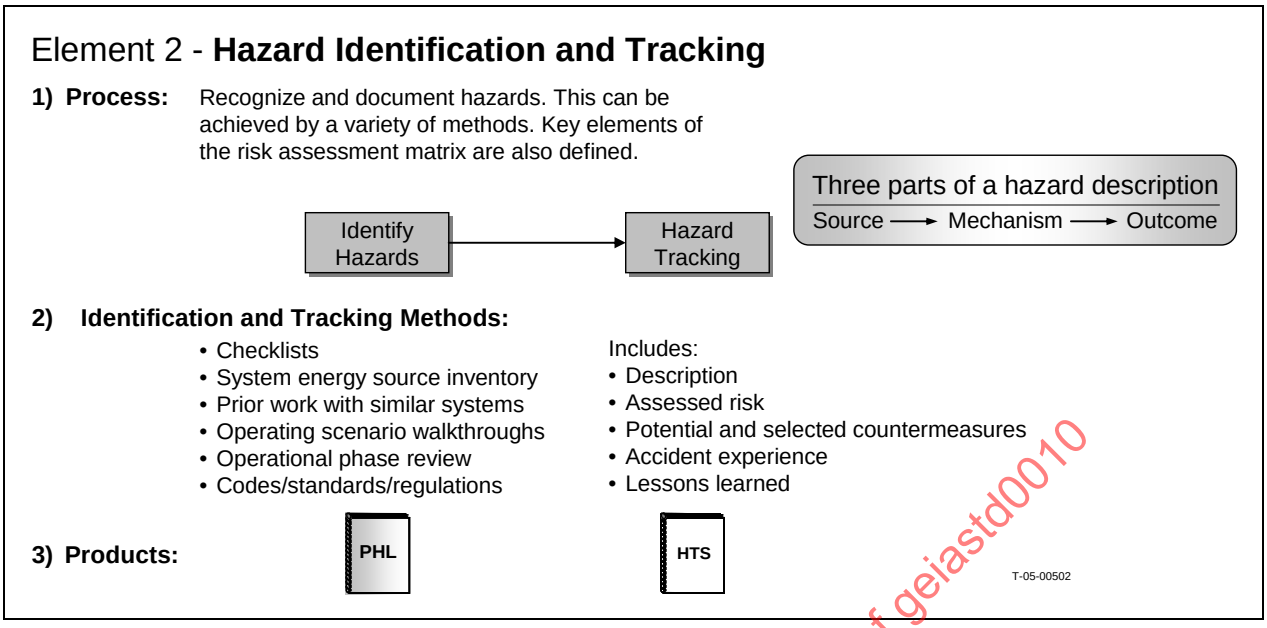


Figure A-3 — Program Element 2—Hazard Identification

A.3.2.1 Identify Hazards

Hazard identification can be achieved by a variety of mutually complementary methods including the use of checklists, prior work with similar systems, and operating scenario walkthroughs. Approaches have been developed and used to identify system hazards. Commonly used approaches for identifying hazards can be found in the reference material listed in Section 2 of this standard. A key aspect of many of these approaches is empowering the design engineer with the authority to design systems whose mishap risk is ALARP and the responsibility to identify to program management the hazards associated with the design. Hazard identification approaches often include using system users in the effort.

A.3.2.2 Describe Hazards

Hazards must be described in terms that identify: a potential source of harm, the mechanism whereby the harm may be caused, and the outcome of the harm itself. Keep in mind that one combination of source and mechanism may have the potential to cause harm to more than one asset, an asset being something of value. Assets include but are not limited to personnel, facilities, equipment, operations, data, the public, and the environment, as well as the system itself. An effective way to deal with these multiple outcomes from one source and mechanism is to treat each outcome, each harmful impact on an asset, as a separate hazard. The importance of this becomes obvious during the risk reduction element (Section A.3.4) when each potential mitigator is identified and its effectiveness in reducing the risk to each asset is weighed against the cost and feasibility of the mitigator. In some cases outcomes may be tightly linked, for instance, “death or serious injury to personnel” is linked to “serious damage to or loss of aircraft” when a hazard mechanism includes aircraft impact with the ground. In this case, these two outcomes might best be treated as components of a single hazard.

A.3.2.3 Track Hazards, Hazard Closure, and Mishap Risk

Maintain a HTS that includes hazard descriptions, mishap severity and probability, hazard causes (which may relate to hardware, software, or human-systems interface), mitigators for each cause, and verification for each mitigator, their closure actions, and mishap risk throughout the system life cycle. The HTS must be maintained throughout the system life cycle.

A.3.2.3.1 Process for Tracking of Hazards and Mishap Risk

Each system must have a current log of identified hazards including an assessment of the mishap risk. As changes are integrated into the system, this log is updated to incorporate added or changed hazards and the associated mishap risk. The Managing authority must formally accept residual mishap risk of system hazards. Users must be kept informed of hazards and mishap risk associated with their systems.

A.3.2.3.2 Program Manager Responsibilities for Communications, Acceptance, and Tracking of Hazards and Mishap Risk

The Developer PM is responsible for maintaining a log of all identified hazards of the system. The Developer PM must communicate known system hazards and associated risk to all system developers and users. As changes are integrated into the system, the Developer PM must update this log to incorporate added or changed hazards and the mishap risk identified by the Developer. The Developer PM is also responsible for informing his team about his expectations for handling of newly discovered hazards. The Developer PM must evaluate new hazards and the resulting mishap risk, and either recommends further action to mitigate the hazards, or formally document the acceptance of these hazards and mishap risk. The Developer PM must evaluate the hazards and associated mishap risk in close consultation and coordination with the Managing authority, to assure that the context of the user requirements, potential mission capability, and the operational environment are adequately addressed. Copies of the documentation of the hazard and risk acceptance are provided to both the Developer and the system user. Hazards for which the Managing authority accepts responsibility for mitigation must also be included in the formal documentation. For example, if the Developer decides to execute a special training program to mitigate a potentially hazardous situation, this approach must be documented in the formal response to the Managing authority. Mishap risk and hazards must be communicated to system test efforts for verification of the effectiveness of risk mitigation.

A.3.3 Element 3 — Risk Assessment

After hazards are identified in Element 2, the identified hazards are reviewed and mishap severities, and probabilities or frequencies are assessed and documented. Figure A-4 shows a simplified version of the risk assessment process. The products of this element may include a PHA, O&SHA, SSHA, SCF list, CSI list, and an SHA.

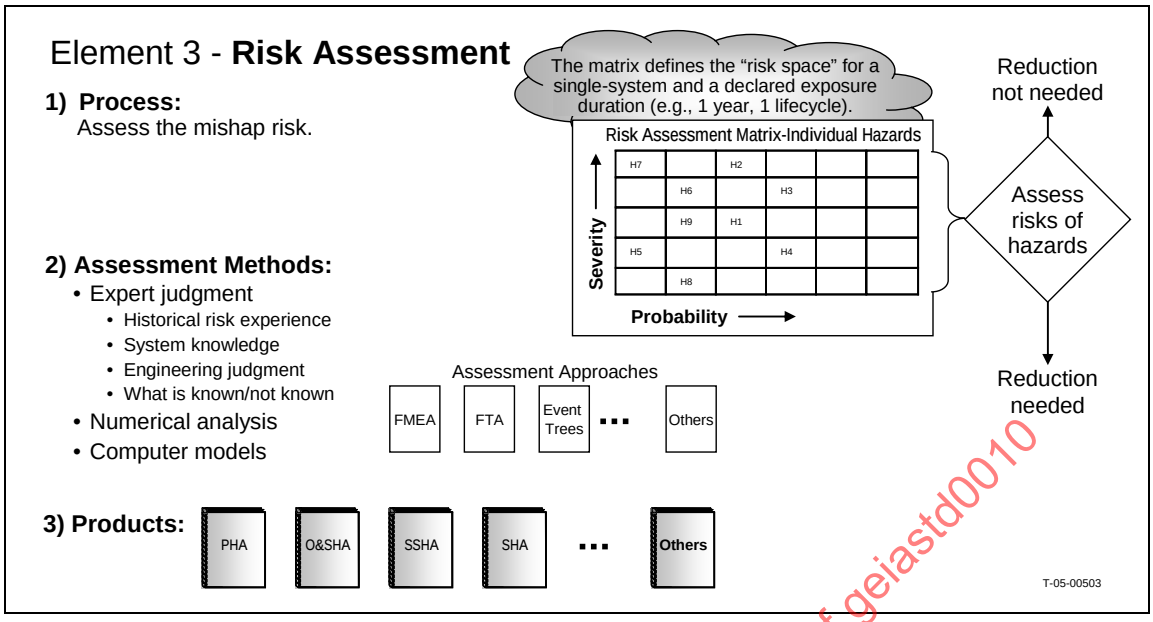


Figure A-4 — Program Element 3—Risk Assessment

A.3.3.1 Risk Assessment Methods

Several methods are available to assess the mishap risk including expert judgment, numerical analysis, computer models, failure modes and effects analysis (FMEA), and fault tree analysis (FTA). Mishap risk assessment matrices described in Section A.5 may be used to assess mishap risk of a hazard in terms of severity, and probability or frequency. For each identified hazard, consider the postulated outcomes to determine the range of severity of the hazard. For each mishap severity category associated with the range of severity, consider the postulated sources, which may relate to hardware, software, or human-systems interface, as well as the likelihood that given sources may lead to applicable outcomes, to assess the mishap probability category. Determine which severity-probability pair has the greatest risk. This pair is the assessed mishap risk of the hazard. If two or more severity-probability pairs are of equal risk then the one with the greatest severity is the assessed mishap risk. Assessing a hazard in terms of one cell of a mishap risk assessment matrix associates the risk with a cell of the matrix but stops short of actually determining the specific loss of assets over the life of the system. If possible, estimate these losses to aid in the analysis of the effectiveness of risk reduction mitigators (Section A.3.4) and to better inform the designated risk acceptance authority who must decide whether to accept residual mishap risk or continue risk reduction efforts. To ensure effectiveness of risk mitigation, the risk assessment process must clearly link each mitigator with the hazard sources and mechanisms to which it applies.

A.3.3.1.1 Mishap Risk Impact

The mishap risk impact is assessed, as necessary, using other factors to discriminate between hazards having the same mishap risk index. One might discriminate between hazards with the same mishap risk index in terms of mission capabilities, or social, economic, and political factors. Program management must closely consult with the using organization on the decisions used to prioritize resulting actions.

A.3.3.1.2 Mishap Risk Assessment Approaches

References for commonly used approaches for assessing mishap risk can be found in Section A.3.3.

A.3.3.2 Assess Software Criticality

For systems with safety critical software (i.e., software controls safety critical functions), each safety critical software function and requirement must be assigned a software criticality index (SCI). Guidance on software safety criticality assessment is provided in Section A.6.

A.3.3.3 Identify Critical Safety Items

A critical safety item (CSI, Task 209)) is defined as a part, subassembly, assembly, subsystem, installation equipment, or support equipment for a system that contains a characteristic, any failure, malfunction, or absence of which could result in mishaps with either catastrophic or critical outcomes. For systems required to have a CSI list, mishap risk assessment will be used to develop that list.

A.3.3.3.1 Functional Hazard Analysis

To identify CSIs, the contractor performs a functional hazard analysis (FHA, Task 208) to identify the safety critical functions (SCF) of the system, then maps the list of SCFs to the design to identify safety critical systems and sub-systems (hardware and software). Hardware items that have critical characteristics that are essential to the SCF are CSIs. A critical characteristic is defined as any feature such as dimension, tolerance, finish, material or assembly, manufacturing or inspection process, operation, field maintenance, or depot overhaul requirement that if non-conforming, missing, or degraded during the life cycle of a CSI, may cause the failure or malfunction of the item. In lieu of an FHA, a failure mode, effects and criticality analysis (FMECA) may also serve to provide the list of CSIs.

A.3.3.3.2 Design Control Activity

The appropriate design control activity approves contractor-developed CSI lists. The design control activity is the systems command of a military department that is specifically responsible for ensuring the military worthiness of a system or equipment. Generating the CSI list is an iterative process that begins when SCFs are identified. The CSI List may be finalized at critical design review but must be provided as timely inputs to supportability and maintenance planning processes. Clear, consistent identification of CSIs is fundamental to ensuring proper priorities, treatment, and controls are implemented throughout the product's life cycle.

A.3.3.4 Total System Risk Consideration

Most hazard analysis techniques are designed to identify and assess the risk of individual hazards, considered one at a time. Risk acceptance authorities, however, must also consider the overall, or total system, risk presented by the system in its entirety. Consideration of total system risk is useful because the aggregation of a number of otherwise acceptable individual risks may present an unacceptable risk when considered in total. Furthermore, the most cost effective approach to lowering a system's total system risk may be to further mitigate an otherwise acceptable individual risk. The program's treatment of total system risk must be identified in the SSMP and/or SSPP.

A.3.4 Element 4 — Risk Reduction

Risk reductions are achieved by understanding the risk drivers, reducing risk according to the system safety mitigation order of precedence, and then reassessing the risks. Mitigators for reducing risk include design changes, engineered safety features, safety devices, warning devices; and procedures or training. Mitigators may serve to eliminate the hazard or reduce severity or probability of potential mishaps. The mitigators for each hazard must be selected based on effectiveness, cost, and feasibility. Feasibility includes consideration of both means and schedule for accomplishment. After mitigators have been selected, the residual mishap risks must be reassessed to ensure that risks are ALARP. Identify potential mishap risk mitigation alternatives and the expected effectiveness of each alternative or method. Be aware that though the risk from a hazard may have been reduced significantly, its assessment may remain in the same cell of the mishap risk assessment matrix. This does not mean a mitigator will not be selected. Hazards must be prioritized so that corrective action efforts can be focused on the most serious hazards first. A categorization of hazards may be conducted according to the mishap risk potential they present. Mishap risk mitigation is an iterative process that culminates when the mishap risk has been reduced to a level as low as reasonably practicable as determined by the appropriate authority. Typical products of this element may include an SAR and hazard reports. The risk reduction element is shown in Figure A-5 and discussed below.

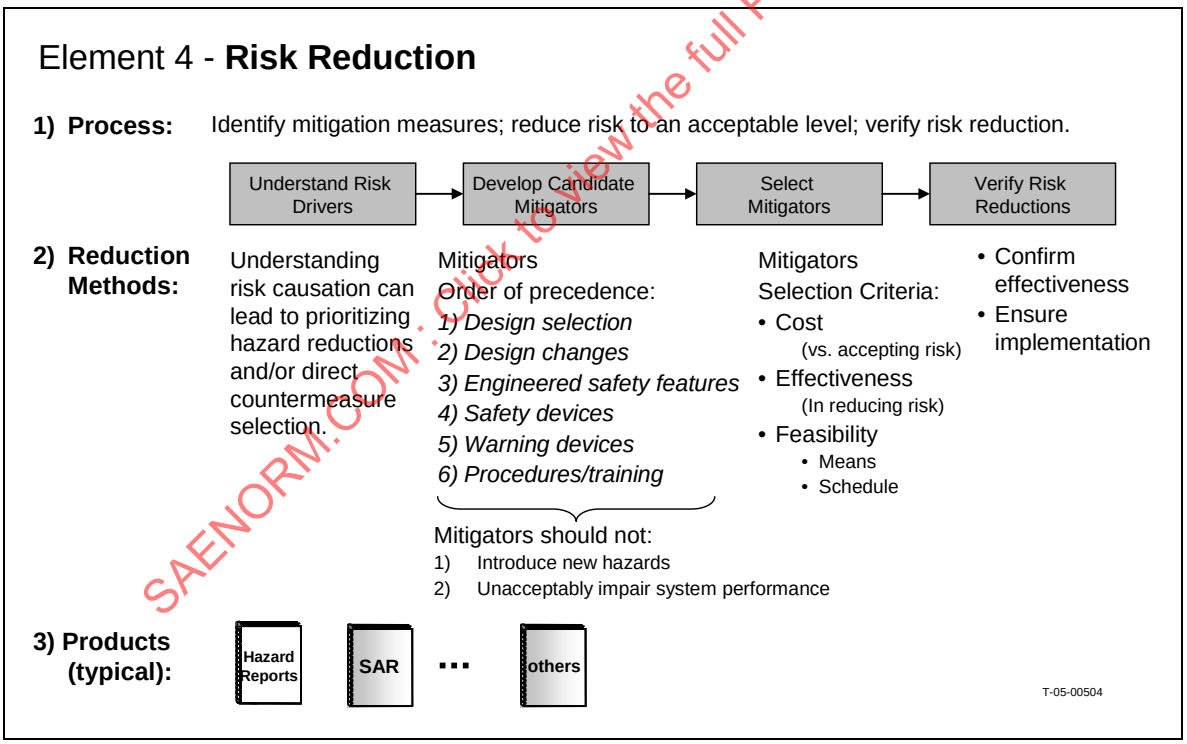


Figure A-5 — Program Element 4—Risk Reduction

A.3.4.1 Understand the Risk Drivers

For the system, determine which hazards are the drivers of the total system risk (R). For each hazard, determine which sources and mechanisms are the drivers of the single hazard risk (r). A good understanding of these risk drivers facilitates effective development, selection and prioritization of risk mitigators.

A.3.4.2 Develop and Document Candidate Mitigators

Identify potential mishap risk mitigators and the expected effectiveness of each. Mishap risk mitigation is an iterative process that culminates when the mishap risk has been reduced to a level ALARP as determined by the appropriate authority. As hazard analyses are performed, hazards must be identified that will require mitigation. The system safety mitigation order of precedence defines the order to be followed for satisfying system safety requirements and reducing risks. Evaluate the alternatives for eliminating the specific hazard or mitigating its risk so that the most practicable mitigators can be implemented. While the relative effectiveness, cost, and feasibility of specific mitigators may vary depending on the hazard, the system safety mitigation order of precedence generally is as follows:

- Eliminate hazard through design selection.
- Reduce mishap risk through design alteration.
- Incorporate engineered safety features (ESF).
- Incorporate safety devices.
- Provide warning devices.
- Develop procedures and training.

A.3.4.2.1 Software Safety Hazard Mitigation

The most effective approach to minimizing safety risk associated with software is to conduct the safety critical requirements analysis (SCRA). The SCRA must be formally communicated with the software development team. An FHA must be conducted to determine the effects on safety critical functions of the system to be commanded, controlled, and monitored by software and to provide the software developer with clear concise derived safety requirements. The software safety analyses (top-level, detail- level, code-level if required) are conducted as an integral part of the hazard analysis processes. Only then can the software contributors to the hazards be understood. The software safety engineer must develop specific safety requirements as part of software requirements to mitigate risk for these software contributors.

A.3.4.2.2 Specific Software Requirements

After the software contributors to hazards are understood, the software safety engineer must develop to mitigate risk for these software contributors. The safety critical requirements must be communicated with the software development team and tracked through the software development lifecycle down to the code and test procedures. The software safety integrity assurance process (see Section A.6) must be used to provide assurance and confidence that the specified safety critical software functionality and requirements have been implemented and verified. Based on completion of all the software integrity assurance activities the software safety engineer can determine a level of confidence that the software will perform as specified and that the associated hazards have been mitigated. The confidence level can be used to perform a final risk assessment, as described in Section A.6.3. IEEE STD 1228 is an existing commercial standard that can be used as a guideline for Software System Safety.

A.3.4.3 Select Mitigators

Reduce the system mishap risk through mitigators mutually agreed to by the Managing authority and the Developer. Mitigators must be selected based on cost, effectiveness, and feasibility.

A.3.4.4 Verify Risk Reductions

Verify mishap risk mitigation through appropriate analysis, testing, and inspection. Mitigators must be evaluated to ensure implementation and confirm effectiveness. Document the assessed residual mishap risk. The Developer PM must ensure through the system test effort that the selected mitigators will produce the expected reduction in mishap risk. New hazards identified during testing must be reported to the Managing authority for further risk reduction efforts.

A.3.4.5 Testing

Mishap risk and associated hazards must be communicated to the system tester to verify mishap risk reduction of the system undergoing testing and ensure that the mishap risk of the testing itself is ALARP.

A.3.4.5.1 Testing to Verify Risk Reduction

Tests and demonstrations must be defined and conducted to verify the effectiveness of selected mitigators. Test or demonstrate safety critical equipment and procedures to determine the mishap severity or to establish the margin of safety of the design. Consider induced or simulated failures to demonstrate the failure mode and acceptability of safety critical equipment. When it cannot be analytically determined whether the corrective action taken will adequately mitigate a hazard, conduct safety tests to evaluate the effectiveness of the mitigators. Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or subscale and model simulation. Integrate testing of safety systems into appropriate system test and demonstration plans to the maximum extent possible.

A.3.4.5.2 Conducting Testing.

The Developer PM must ensure that test teams are familiar with unique mishap risks of the system. Review test plans, procedures, and previous test results for all tests including design verification, operational evaluation, production acceptance, and shelf-life validation to ensure that testing will be conducted with mishap risk ALARP. Mitigate all known system hazards plus any additional hazards introduced by test procedures, instrumentation, hardware, and environments.

A.3.4.5.3 Communication of New Hazards Identified During Testing

Testing organizations must ensure that hazards and safety discrepancies discovered during testing are documented and communicated to the Managing authority.

A.3.5 Element 5 — Risk Acceptance

The designated risk acceptance authority determines whether or not the mishap risks have been reduced to ALARP within the constraints of operational effectiveness and suitability, time, and cost (or that the risk is acceptable). Figure A-6 depicts the risk acceptance element. Review and acceptance of each interim and residual single hazard risk (r) by the appropriate authority is a necessary action in the risk management process. Consideration must also be given to requiring the review and acceptance of total system risk (R) by the appropriate authority. The designated risk acceptance authority must be kept informed regarding identified hazards and mishap risks.

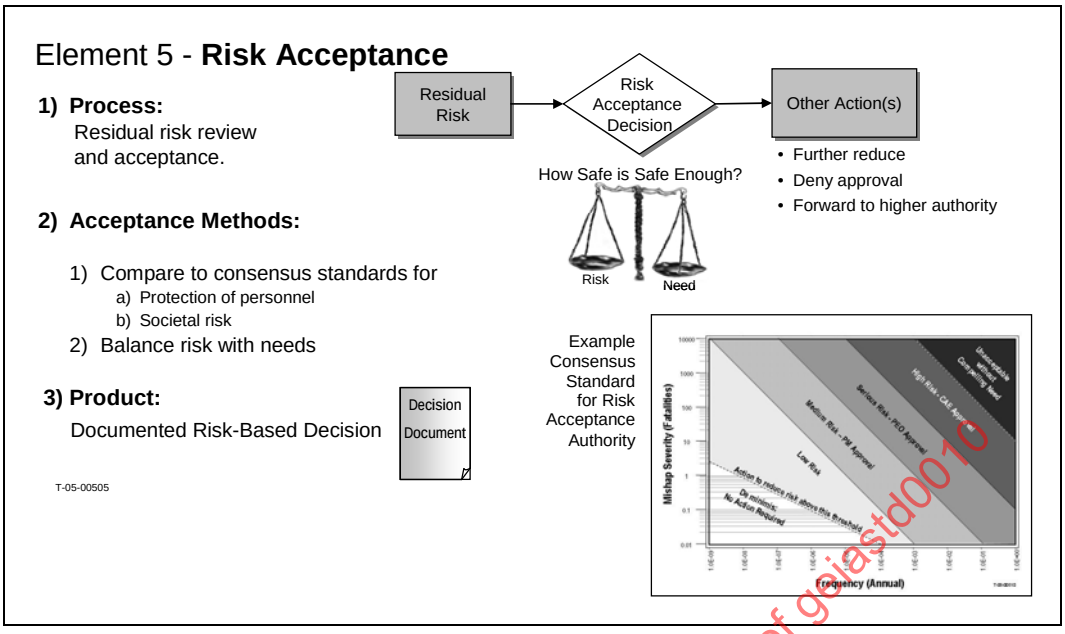


Figure A-6 — Program Element 5 – Risk Acceptance

A.3.5.1 Review of Hazards and Acceptance of Mishap Risk by the Designated Authority

The Developer PM must know what interim and residual mishap risks exist in the system being delivered. The Managing authority provides resources to the Developer to mitigate hazards with significant mishap risk. The Developer PM is obligated to report serious risk hazards to the Managing authority who must then either accept the risk or take action and allocate additional resources to reduce the risk.

A.3.5.2 Verify Review and Acceptance

The Managing Authority is responsible for formally documenting the acceptance of interim and residual mishap risks of the system by the appropriate authority. The developer must reassess the risk of hazards whenever there are any changes or modifications to the system or its use. The developer and managing authority organization must agree on the assessed level of mishap risk prior to acceptance of the risk by the risk acceptance authority.

A.3.5.3 Accept Interim and Residual Mishap Risk

Residual risk is the mishap risk that remains after all planned mitigators have been implemented. Interim risk is that risk that is present until planned mitigating actions have taken place. There must be documentation of the mishap risk acceptance along with substantiation that mishap risk has been reduced as low as is reasonably practicable.

A.4 Specific Requirements

The Developer must ensure that all types of hazards are identified, evaluated, and mitigated to a level compliant with acquisition management policy (federal, international, and state) laws and regulations, executive orders, treaties, and agreements. The Developer must:

- Establish, plan, organize, implement, and maintain an effective system safety effort that is integrated into all life cycle phases.
- Ensure that system safety planning is documented to provide all program participants with visibility into how the system safety effort is to be conducted.
- Establish definitive safety requirements for the development, procurement, and sustainment of the system. The requirements must be set forth clearly in the appropriate system specifications and contractual documents.
- Provide historical safety data.
- Monitor the system safety activities, and review and approve delivered data in a timely manner, if applicable, to ensure adequate performance and compliance with safety requirements.
- Ensure that system specifications are updated to reflect results of safety analyses, tests, and evaluations.
- Evaluate new lessons learned for inclusion into appropriate databases and submit recommendations to the responsible organization.
- Establish system safety teams to assist in developing and implementing a system safety effort.
- Provide technical data to enable the Developer to accomplish the defined tasks.
- Document acceptance of hazard risk assessments.
- Ensure users are appropriately notified or warned of identified system hazards and mishap risk.
- Ensure the program meets the intent of this Standard Practice.
- Ensure adequate resources are available to support the program system safety effort.
- Ensure that the system safety technical and managerial personnel are qualified for the job.

A.5 Example Mishap Risk Assessment Matrices

This section contains seven examples to show a spectrum of potential uses for the mishap risk assessment matrix. Mishap risk assessment matrices are used to assess risks and also to determine who will accept risks. They may also serve as a useful tool to combine the individual risks into a total system risk for the system. With this in mind, a well-designed mishap risk assessment matrix must have the following features:

a. Mishap risk assessment matrices must be tailored to each system or class of systems based on the expected range of severity of potential mishaps and the range of probability or frequency of these mishaps.
b. Orient the severity and probability (or frequency) axes so that one axis increases upward and the other increases to the right in accordance with the Cartesian coordinate system. Since René Descartes first developed this system in 1637, mathematicians, scientists and engineers have been trained to use this graphical orientation of data. It greatly reduces confusion to orient the axes in this way.
c. Use logarithmic scales on each axis with logical and proportional ranges for mishap severity categories and mishap probability categories. This assures that the risk, which is a product of probability and severity, will also be proportional.
d. Assign the four levels of decision authority for risk acceptance (high, serious, medium, low) to each cell of the matrix. Bear in mind that if the first three features described above are in place, a cell will have the same level of risk as the cell diagonally up and to the left, and the cell diagonally down and to the right.

The following sections fully implement these features.

A.5.1 Example 1: Mishap Risk Assessment Matrices

Programs using mishap risk assessment matrices from other standards may not contain all desirable features. Tables A-2 through A-5 describe typical risk matrices.

A.5.1.1 Mishap Severity

Mishap severity categories are defined to delineate ranges of mishap outcomes in terms of fatalities, injuries, property damage, or other loss. Example mishap severity categories are shown in Table A-2. The dollar values shown in this table must be established on a system-by-system basis based on the highest severity mishap of the system and the lowest severity mishap that could be of concern.

Table A-2 — Example – Mishap Severity Categories

Description	Category	Environmental, Safety, or Health Result Criteria
Catastrophic	I	Could result in death, permanent loss of system function, permanent total disability, or loss exceeding $1M.
Critical	II	Could result in major system damage, permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, or loss exceeding $200K but less than $1M.
Marginal	III	Could result in minor system damage, injury or occupational illness resulting in one or more lost work days, or loss exceeding $20K but less than $200K.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, or loss exceeding $2K but less than $20K,

NOTE: These mishap severity categories provide guidance to a wide variety of programs. Other severity definitions may be used.

A.5.1.2 Mishap Probability or Frequency

Mishap probability is the likelihood of mishap occurrence over a standard or customer-defined exposure interval. Probability is mathematically between zero and one. Mishap frequency is the rate of mishap occurrence. Frequency is sometimes substituted for probability as a component of risk. Mishap probability categories delineate ranges of mishap probabilities described in terms probability of one or more mishaps in a specified exposure interval or they delineate ranges of mishap frequency described in terms of occurrences per unit of time, events, population, items, or activity. If unable to quantify probability or frequency, mishap probability categories are defined in terms of subjective descriptors (see Table A-3 and Table A-6). Assigning a quantitative mishap probability or frequency to a potential design or procedural hazard is sometimes difficult due to lack of data. In this situation, a mishap probability or frequency may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability or frequency is documented in hazard analysis reports. Example quantitative and subjective mishap probability categories are shown in Table A-3, Table A-6, and Figures A-7 through A-11.

Table A-3 — Example – Mishap Probability Categories

Description*	Level	Specific Individual Item	Fleet or Inventory**
Very Likely	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Likely	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} and greater than 10^{-2} in that life.	Will occur frequently.
Probable	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} and greater than 10^{-3} in that life.	Will occur several times.
Unlikely	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} and greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur.
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.
Impossible	F	Incapable of occurrence. This category is used when potential hazards are identified and later eliminated.	

* Definitions of descriptive words may have to be modified based on quantity of items involved.
** The expected size of the fleet or inventory must be defined prior to accomplishing an assessment of the system.

A.5.1.3 Mishap Risk Assessment

Mishap risk classification in terms of mishap severity and mishap probability (or frequency) can be performed by using a mishap risk assessment matrix. An example of a mishap risk assessment matrix is shown at Table A-4. Using the matrix to assess the risk for a hazard, the analyst selects the matrix cell representing the levels of combined severity and probability of outcome for which risk is greatest. This is repeated for each individual asset threatened by the hazard (personnel, equipment, etc.). For a hazard having a range of outcome severity covering more than one mishap severity category, the severity-probability pair representing the greatest risk is selected as the assessed mishap risk of the hazard for that asset. If two or more severity-probability pairs are equal as representing the greatest risk for a given asset, the declared mishap risk is given by the pair having the greatest severity. In this example matrix, the assessed severity-probability pair is designated by the Roman numeral and letter corresponding to the mishap severity category (from Table A-2) and the mishap probability category (from Table A-3), e.g., I/D, IV/B, etc. Some matrices (Examples 3 and 5) use Arabic instead of Roman numbers (e.g., 1/D, 4/B, etc.). Also in this example, each cell of the matrix is assigned a number called a mishap risk index (Table A-4). Mishap risk indices can be used to rank order hazards according to their mishap risks.

Table A-4 — Example – Mishap Risk Index Values

PROBABILITY / SEVERITY		Very Likely A	Likely B	Probable C	Unlikely D	Improbable E	Impossible F
I	Catastrophic	1	2	4	8	12	NA
II	Critical	3	5	6	10	15	
III	Marginal	7	9	11	14	17	
IV	Negligible	13	16	18	19	20	

A.5.1.4 Mishap Risk Categories

In this example, mishap risk indices are used to group individual hazards into mishap risk categories. Table A-5 includes a listing of mishap risk index, mishap risk category and mishap risk acceptance level as system management might assign them. Mishap risk acceptance is discussed in Section A.3.5. The using organization must be consulted by the corresponding levels of program management prior to mishap risk acceptance.

Table A-5 — Example – Mishap Risk Acceptance Levels (MRALs)

Mishap Risk Index	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Managing Authority
6 – 9	Serious	Managing Authority
10 – 17	Medium	Program Manager
18 – 20	Low	Program Manager

A.5.2 Example 2: Mishap Risk Assessment Matrix

Figure A-7 is four-by-five matrix. It features logarithmic probability (frequency) scales. The severity scale is based on mishap class. It assigns numbers to the matrix cells in their order of decreasing risk. This allows comparisons of relative cell-by-cell risks.

Hazard Categorization		Severity			
		Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequency	Frequent (A) = or > 100/100k Hrs	1	3	7	13
	Probable (B) 10-99/100k Hrs	2	5	9	16
	Occasional (C) 1.0-9.9/100k Hrs	4	6	11	18
	Remote (D) 0.1-0.99/100k Hrs	8	10	14	19
	Improbable (E) = or < 0.1/100k Hrs	12	15	17	20

Unacceptable	Managing authority Acceptance 1-5 HIGH SAFETY RISK	Acceptable With Review	Program Manager or Designee Acceptance 11-17 LOW SAFETY RISK
Undesirable	Managing authority Acceptance	Acceptable Without Review	Program Manager or Designee 18-20 VERY LOW SAFETY RISK

Severity

Catastrophic –> $1M / fatality / permanent total disability)
Critical –($200K < damage < $1M / permanent partial disability / hospitalization of 5 or more personnel)
Marginal –($10K < damage < $200K / injury results in 1 or more lost workdays)
Negligible – All other injury/damage

Probability of occurrence for discreet events may replace Frequency based upon the chart below.

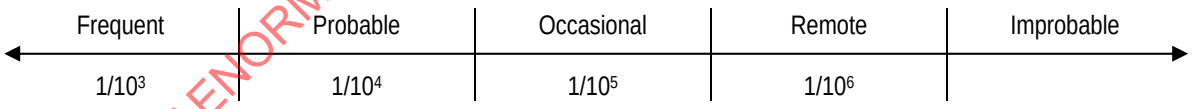
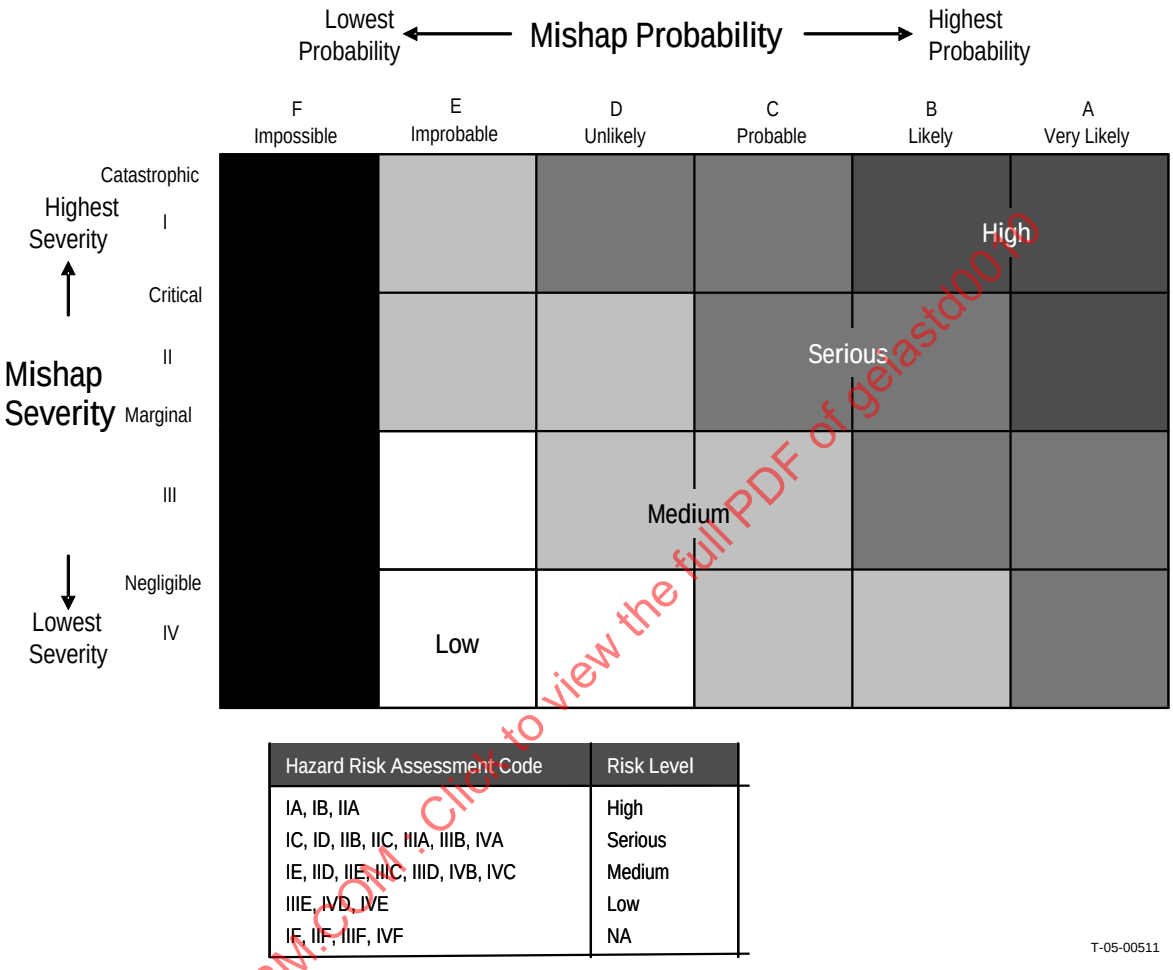


Figure A-7 — Mishap Risk Assessment Matrix

A.5.3 Example 3: Generic Subjective Mishap Risk Assessment Matrix

Figure A-8 is intended to illustrate the major components and methods of a tailored risk assessment matrix.



Hazard Risk Assessment Code	Risk Level
IA, IB, IIA	High
IC, ID, IIB, IIC, IIIA, IIIB, IVA	Serious
IE, IID, IIE, IIIC, IIID, IVB, IVC	Medium
IIIE, IVD, IVE	Low
IF, IIF, IIIF, IVF	NA

Figure A-8 — Generic Subjective Mishap Risk Assessment Matrix

A.5.3.1 Tailoring Process

As part of tailoring, the highest and lowest severity must be specified to establish the severity range. The range in Figure A-8 has been divided into subdivisions. Similarly, the probability scale has been subdivided into equal parts. This four-by-six matrix serves the purpose of bounding, guiding, and displaying. The table below the matrix defines the low, medium, serious, and high risk areas and lists the appropriate decision authorities for each level of mishap risk.

A.5.3.2 Matrix Axis Scaling

Matrix axis scaling may be either subjective, using key phrases to guide judgment as to levels of severity and probability, or quantitative, using numbers.

A.5.3.2.1 Subjective Scaling

Severity and probability axes of the mishap risk assessment matrix can be scaled to guide subjective assessments of risk. For example, Figure A-8 could be used for subjective scaling where levels of mishap severity are ranked from negligible (IV) to catastrophic (I). The mishap probability scale has been similarly treated, with probability categories ranging from impossible (F) to very likely (A). The terms associated with the mishap probability scale represent likelihood rather than the importantly different concept of frequency. Phrases to guide the selection of the subjective terms for probability appear in Table A-6.

Table A-6 — Example – Mishap Probability Categories

Level	Descriptive Word*	Defining Phase *
A	Expected	Approaching certainty
B	Near Expectation	Moderately certain
C	Highly Probable	A near expectation
D	Very Likely	Quite probable
E	Likely	Somewhat certain
F	Probable	Neither surprising nor assured
G	Unlikely	Conceivable, but not expected
H	Improbable	Approaching incredibility
I	Impossible	Incapable of occurring

* Probability statements, although dimensionless, must relate to an expressed interval of item or system exposure, e.g.: a specified number of hours of operation, cycles of use, miles driven, man-hours worked, missions completed.

A.5.3.2.2 Quantitative Scaling

Subjective expressions for severity and probability (“Frequent,” “Occasional,” “Critical,” etc.) are of limited precision. Varying interpretations of the terms can lead to substantial dispute over assessments of severity and probability. Therefore, when assessing risk, use numerical expressions of severity and probability along with similarly quantitative scaling of the risk matrix axes if possible. Logarithmic scaling of quantitatively distributed values along the axes of the risk assessment matrix is to be preferred. This means major scale indices increase stepwise not by single integers (e.g., 1, 2, 3, …) but by factors of ten, called orders of magnitude (e.g., …10^{-7}, 10^{-6}, 10^{-5}, 10^{-4}… or…1, 10, 100…or …2, 20, 200…). The scale steps could also increase by two orders of magnitude (…10^{-8}, 10^{-6}, 10^{-4}, 10^{-2}, 1, 100, 10,000…) or half orders of magnitude (10^{-7}, $10^{-6.5}$, 10^{-6}, $10^{-5.5}$…1, 3.16, 10, 31.6, 100, 316…). Adjusting the scales in this way adjusts the resolution capability of the matrix. Resolution is determined by the size of the smallest calibrated increment in mishap severity and probability (or frequency) categories. Examples 3, 4, and 5 are at one order of magnitude resolution. Example 6 is at one-half order of magnitude resolution. Matrix scale resolution must not be made finer than is justified by the quality of the data to be displayed nor less than is needed to express data values serving a practical use.

A.5.4 Example 4: Multi-Purpose Aircraft Mishap Risk Assessment Matrix

Figure A-9 is nine-by-seven matrix intended for multiple aircraft systems. It features logarithmic scales and can be varied in size based on the maximum severity mishap of the system. The mishap severity categories are numbered in reverse of the other examples to enable uniform reporting of risk regardless of how large or small the matrix is tailored.

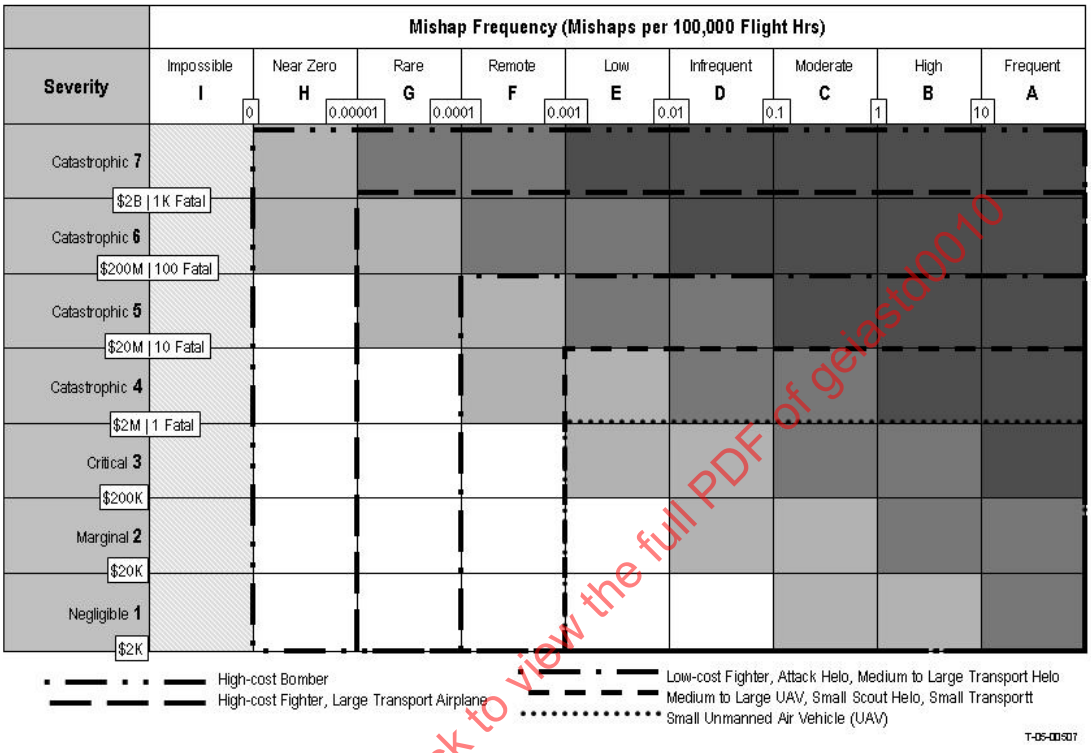


Figure A-9 — Example Multi-Purpose Aircraft Family Mishap Risk Assessment Matrix

A.5.5 Example 5: Single Order of Magnitude Resolution Mishap Risk Assessment Matrix

Figure A-10 is an eight-by-six matrix proposed for use with low probability and high consequence hazards. It features logarithmic scales and four levels of decision authority. This matrix is designed for use where risk for most hazards has been assessed subjectively, yet the scaling of each axis remains useful for summing total system risk.

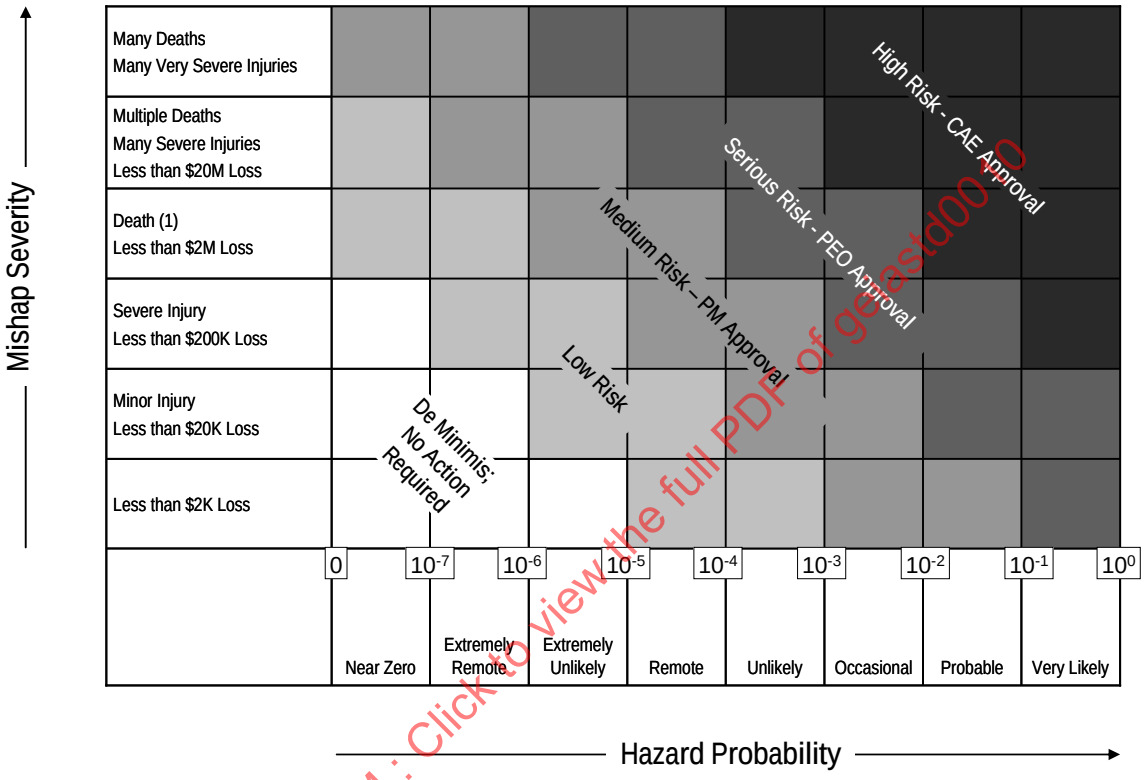


Figure A-10 — Example Single Order of Magnitude Resolution Mishap Risk Assessment Matrix

A.5.6 Example 6: Half Order of Magnitude Mishap Resolution (14 x 14) Risk Assessment Matrix

Figure A-11 is a half order of magnitude mishap risk assessment matrix that may be desirable where quantitative risk assessment (QRA) or other quantified methods are used in quantifying risk. It features a resolution of half orders of magnitude in both dimensions. The consequence scale is quantified in terms of fatalities, serious injuries, and dollars lost. QRA methods may also be used with matrices having scales with full order or magnitude scale markings.

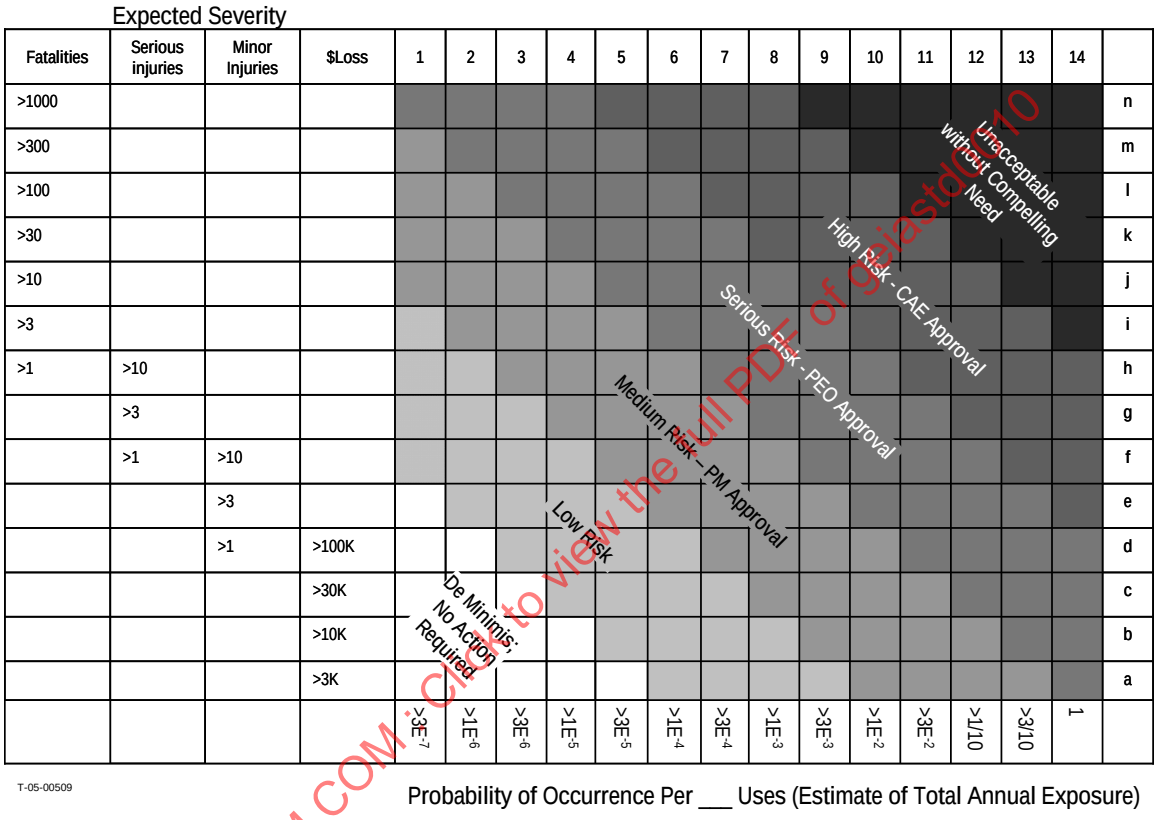


Figure A-11 — Example Half Order of Magnitude Resolution Mishap Risk Assessment Matrix

A.5.7 Example 7: Total System Risk Assessment Criteria

Where total system risks are calculated, the traditional method of plotting risks on a mishap risk assessment matrix may prove unsatisfactory. Another method in common use is to establish criteria plotted as “iso-risk” lines using the same severity and probability scales that define matrices. Published criteria defining “how safe is safe enough?” may be used to define these lines; however, this may differ for each system type. This approach may be used for comparison of single hazard risks, or total system risk. Figure A-12 is an example of potential total system risk assessment criteria.

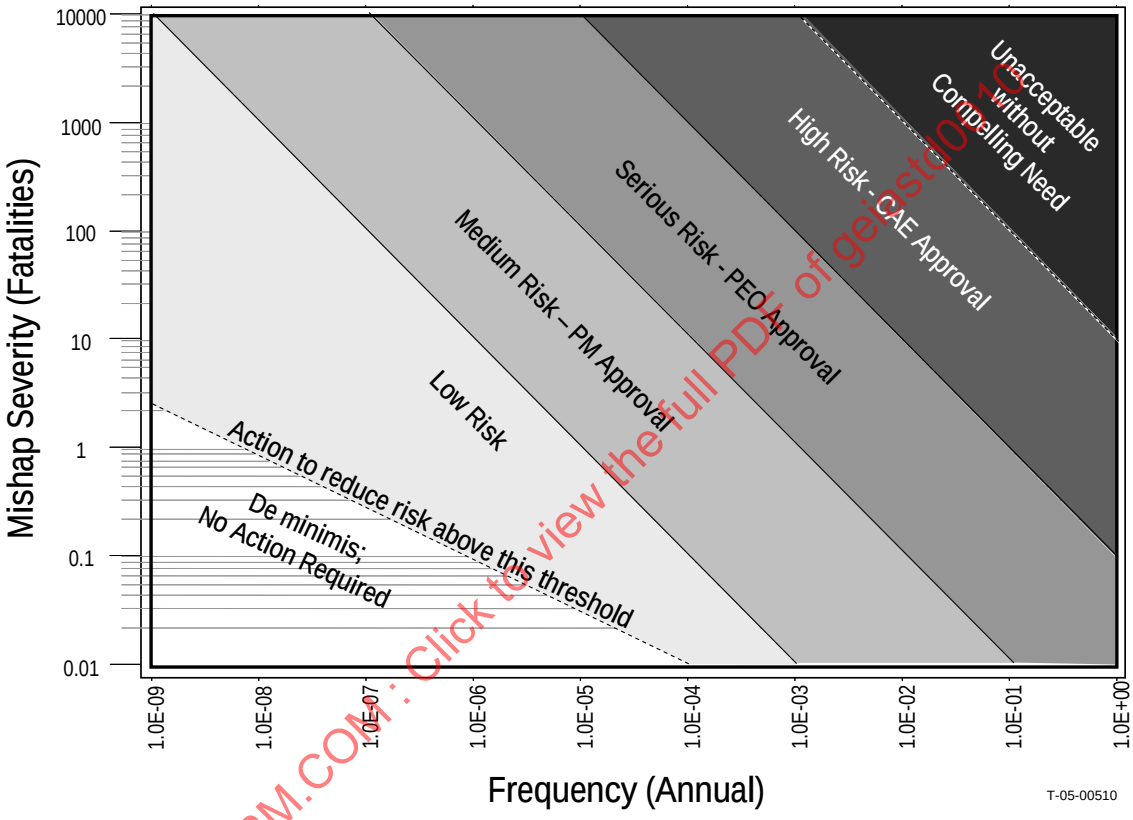


Figure A-12 — Example Total System Risk Assessment Criteria

A.5.7.1 Total Risk Criteria

The example was developed using risk acceptance criteria that have been previously published, and the numerical values shown could be varied to fit the class of system. This approach may be tailored for use with single hazard risks (r) or total system risk (R). The chart plots iso-risk lines on the diagonal. For example, the line extending from 10000 on the severity axis to $1x10^{-3}$ on the probability axis represents an iso-risk expectancy of one fatality per year for the total system. The chart could be useful in advising decision makers when the total system risk is above a certain iso-risk threshold.

A.5.7.2 Decision Making Areas

The system risk assessment criteria are also divided into six decision-making areas associated with the appropriate level of acceptance authority.

a. *De minimis*. This approach uses a straight line to define the *de minimis* threshold for the system safety program. Below this level, a hazard does not warrant any additional expenditure of mitigation resources.
b. Low risks. These risks are high enough to expend resources to reduce. Residual mishap risk must be accepted.
c. Medium risks. These risks are high enough to warrant some concern. Residual mishap risk acceptance is necessary.
d. Serious risks. These risks require risk acceptance at a senior management level.
e. High risks. These risks require risk acceptance at the highest management or Customer level.
f. Unacceptable risks. These risks are unacceptable without a compelling need.

A.5.8 Example Measures of Total System Risk

To evaluate a system against the criteria in Section A.5.7.1, a measure of system risk (R) is needed. The format of Figure A-12 dictates that this measure must provide both a measure of severity and a measure of probability of occurrence to plot the system risk. These measures assume summed hazards are totally independent. Valid measures of total system risk might be, for example:

a. Expected loss rate. This measure computes the severity component as the average loss per system exposure interval that would be realized if numerous copies of the system were operated for numerous life cycles. The probability to be plotted is a value of 1.0 since this method estimates the level of loss that, on average, will happen every time the system is operated for the specified exposure interval.
b. Maximum loss. This measure assigns the severity component to be plotted as the level of loss corresponding to the most severe single hazard. The probability of maximum loss is computed by dividing the expected loss rate by the maximum loss level.
c. Most probable loss. To plot this measure, sum the probabilities of hazards at each level of severity. The severity level with the highest probability is the most probable loss. Plot this severity level with a probability computed by dividing the expected loss rate by the most probable loss level.
d. Conditional loss rate. The probability value is the sum of the probabilities for all hazards. The severity value is the conditional expected loss and is computed by dividing the expected loss rate by the value of the summed probabilities. The result displays the probability that a mishap will occur, and the expected amount of the loss, given that a mishap does occur.

A.6 Software System Safety Engineering Analysis and Integrity

A successful software safety engineering activity is based upon both a hazard analysis process and a software integrity process. Emphasis is placed on the context of the "system" and how software contributes to failures, hazards, and/or mishaps. From the perspective of the system safety engineer and the hazard analysis process, software is considered as a subsystem. In most instances, the system safety engineers must perform the hazard analysis process while the software development, software test, and independent verification and validation (IV&V) team(s) implement the software integrity process. The hazard analysis process is an activity that identifies and mitigates the exact software contributors to hazards. The software integrity process increases the confidence the software will perform as specified (i.e., to software performance requirements) while reducing the number of contributors to hazards that may possibly exist in the system. Both processes are essential to reduce the likelihood of software initiating a propagation pathway to a hazardous condition or mishap.

A.6.1 Software System Safety Engineering Analysis

System safety engineers performing the hazard analysis for the system (PHA, SSHA, SHA, FHA, O&SHA, and HHA) must accomplish the software safety engineering analysis tasks. These tasks ensure that software is considered in its contribution to mishap occurrence. These tasks are well defined and common to most system safety programs. In general, software functionality that directly or indirectly contributes to mishaps, such as the processing of safety critical data or the transitioning of the system to a state which could directly lead to a mishap, must be thoroughly analyzed. Software sources and/or specific software errors that cause or contribute to hazards must be identified at the software module and functional level (functioning out-of-time or out-of-sequence, malfunctions, degrades in function, or does not respond appropriately to system stimuli). In software-intensive, safety-critical systems, mishap occurrence will likely be caused by a combination of hardware, software, and human errors. These complex initiation pathways must be analyzed for the purpose of identifying hazard mitigation requirements and constraints to the hardware and software design and test teams. As a part of the functional hazard analysis (FHA, Task 208) software functionality which has been identified to cause, contribute to, or influence a hazard that could result in a major mishap must be identified as safety critical. Software requirements that implement safety critical functions must also be identified as safety critical.

A.6.2 Software Safety Integrity

Software developers and testers play a large role in producing safe software. Their contribution can be greatly enhanced by the incorporation of a software safety integrity process within the software development plan (SDP) and task activities. The software safety integrity process is based upon the identification and establishment of specific software development and test tasks for each acquisition phase of the software development life cycle (requirements, preliminary design, detailed design, code, unit test, unit integration test, system integration test, and formal qualification testing). All software safety integrity tasks must be performed at an appropriate level of rigor based upon the safety criticality of the software functions within each software configuration item or software module of code. The software safety integrity tasks are defined by performing an FHA to identify safety critical functions (SCF); assigning a software control category (SCC) to each of the software-related safety critical functions; assigning a software criticality index (SCI), software assurance level (SwAL) or software integrity level (SIL); and

the implementation of tasks for each SCF based upon the (SCI). These software safety integrity tasks are further explained in the subsequent paragraphs.

A.6.2.1 Perform a Functional Hazard Analysis

Identify the SCF of the system (see Task 208). Once identified, each SCF is assessed and categorized against the software control categories to determine the level of control of the software over safety-related functionality. Each SCF is mapped to its implementing computer software configuration item (CSCI) or module of code for traceability purposes.

A.6.2.2 Perform a Software Criticality Assessment for Each SCF

The software criticality assessment must not be confused with mishap risk. “Mishap risk” is a measure of the severity and probability of occurrence of a mishap from a particular hazard whereas software criticality is used to determine how “critical” a specified software function is with respect to the safety of the system. The software criticality assessment combines the mishap severity category from the mishap risk assessment with the SCC to derive an SCI as shown in the example software criticality matrix in Table A-7. The SCI is then used as a part of the software integrity assurance process to determine the amount of analysis and testing required for verification of that specific software requirement/function. The SCCs are defined in the bottom section of Table A-VII.

Table A-7 — Example – Software Criticality Matrix

Mishap Severity Category	Software Control Category IV	IIIb	IIIa	IIa/IIb	I
I Catastrophic	(5) NSC	(3) Medium	(2) Serious	(1) High	(1) High
II Critical	(5) NSC	(3) Medium	(3) Medium	(2) Serious	(1) High
III Marginal	(5) NSC	(4) Low	(4) Low	(3) Medium	(3) Medium
IV Negligible	(5) NSC	(4) Low	(4) Low	(4) Low	(4) Low

T-05-00515

SW Criticality Index	Suggested Criteria
(1) High	Requires requirements analysis, in-depth design and code analyses, and in-depth safety specific testing.
(2) Serious	Requires requirements analysis, some design and code analyses, and in-depth safety specific testing.
(3) Medium	Requires requirements analysis, some design and code analyses, and safety specific testing.
(4) Low	Requires safety-critical requirements be identified and tracked, developer follows normal development processes, and some safety specific testing.
(5) Not Safety Critical (NSC)	No safety specific analyses or testing required.

Software Control Categories

I Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence.

IIa Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.

IIb Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the hazard's occurrence.

IIIa Software item issues commands over potentially hazardous hardware systems, subsystems or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.

IIIb Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.

IV Software does not control safety critical hardware systems, subsystems or components and does not provide safety critical information.

A.6.2.2.1 Software Criticality Matrix Tailoring

The software criticality matrix can, and will, be tailored for any given program. An SCI of “1” from the matrix implies that the assessed software function or requirement is very critical to the safety of the system and requires more design and test rigor than software which is less critical. Software with an SCI of “2” to “4” is less critical and requires less design and test rigor than high-criticality software. Unlike the hardware related mishap risk index, a low index number does not imply that a design is unacceptable. Rather, it indicates that greater resources need to be applied to the analysis and testing of the software and its interaction with the system. NOTE: The software criticality index matrix does not consider the likelihood of a software-caused mishap occurring in its initial assessment. However, through the successful implementation of a software safety integrity process, the likelihood of software contributing to a mishap can be greatly reduced.

A.6.2.3 Software Integrity Assurance Matrix (SIAM)

Once SCFs are identified and assessed against the SCC and assigned an SCI (all accomplished thus far by the system safety engineer but agreed upon by the software developers and testers), the implementing software must be designed, coded, and tested against software safety integrity criteria as shown in the SIAM. These criteria must be defined, negotiated, and documented in the SDP and the software test plan (STP) early in the development life cycle.

A.6.2.3.1 SCI Assignment

An SCI (1 High, 2 Serious, 3 Medium, or 4 Low) must be assigned to each safety critical software function and the associated safety critical software requirements. Assigning the SCI value of 5-NSC (not safety critical) to non-safety critical software requirements provides a record that functionality has been assessed and deemed NSC. Individual safety critical software requirements that track to the software hazard reports must be assigned an SCI. The intent of the SCI value of 4 (“Low”) is to ensure that requirements corresponding to this level are identified and tracked through the system. These “low” safety critical requirements only need the normal reviews, analyses, and testing specified by the Developer’s standard software development processes.

A.6.2.3.2 Example SIAM

Table A-VIII depicts an example of what can be placed in the SIAM. It must be noted that an SIAM will be tailored for each individual system or system of systems based upon its complexity, safety criticality, available resources, and value added. To assist in filling out the matrix the following example design requirements and tasks are provided for consideration in Section A.6.2.4 below, and its subparagraphs.

Table A-8 — Example – Software Integrity Assurance Matrix

*****FOR EXAMPLE PURPOSES ONLY***** **Software Integrity Assurance Task**	Criticality Rating			
	(1) High	(2) Serious	(3) Medium	(4) Low
General				
Peer Reviews of all development artifacts are conducted at each phase (requirements, design, code, and test).	M	M	R	R
All design and software components containing safety critical functionality are identified as safety critical and linked to the appropriate software requirements specification (SRS) requirement(s).	M	M	R	R
All safety critical functions and components are documented and linked to the individual hazards identified in the hazard analysis	M	M	M	R
Requirements Analysis Phase				
Independent analysis/verification of algorithms, limits, ranges, critical values, rate, units, frequency and volume via independent evaluation.	M	R	R	NR
Traceability of safety critical requirements from hazard analyses to SRS, software design, code, and test.	M	M	M	R
All safety critical software requirements are broken down to their lowest level and linked to their higher level requirement.	M	M	R	R
All safety critical software requirements are analyzed for verifiability, testability and potential confliction with other requirements.	M	M	R	R
All safety critical requirements are evaluated for timing, resource utilization and throughput.	M	M	M	R
Use of defined Safety related Requirements Guidelines.	M	M	R	NR
Architectural and Detailed Design Phase				
Evaluate safety related components for reliability, maintainability, understandability and performance.	M	M	M	R
Peer reviews of software units identified as safety critical will require the attendance of a reviewer independent from the Software Development Team.	M	M	M	R
For all safety critical requirements ensure that there are no common cause failures between components (i.e., Fault Tree Analysis).	M	M	R	R
For all safety critical components, identify any or all dependencies	M	M	R	R
Verify accuracy and correctness of all algorithms in safety critical components.	M	M	M	M
Verify that all data used in safety critical components are used as specified and are consistently used between components.	M	M	M	R
Verify all interfaces between safety critical components.	M	M	M	R
Evaluate feasibility of safety critical design constraints.	M	M	R	R
Evaluate partitioning of safety critical software (goal is to minimize the number of safety critical components).	M	M	M	R
Coding Phase				
Conduct a safety critical function code review (with safety engineering attendance)	M	M	R	R
Conduct an independent verification of: safety critical algorithms for accuracy, correctness, and boundary values; data consistency between components; and use of defined safety critical guidelines.	M	M	M	R
Software coding standards will require that software units that satisfy safety critical requirements be identified as safety critical.	M	M	M	M
Safety critical software units must be evaluated for logic, data, and interface errors.	M	M	M	M
Algorithms and mathematical computations must be analyzed and tested for accuracy and correctness.	M	M	M	M

****FOR EXAMPLE PURPOSES ONLY**** Software Integrity Assurance Task	Criticality Rating			
	(1) High	(2) Serious	(3) Medium	(4) Low
Testing Phase				
Create a set of unit, unit integration, and software qualification test cases for testing all the logic paths and all statements in the software. Complete coverage testing.	M	M	M	R
At a minimum, unit test cases must exercise each line of executable source code at least once and ensure there is no unused or dead code in the software.	M	M	M	M
For safety critical requirements that are time dependant, timing tests must be included at the unit level.	M	M	M	M
For safety critical requirements, boundary value testing must be performed to validate values at or near the limits of the valid range of their values.	M	M	M	R
White box testing to verify that every code loop is executed the correct number of times and for every possible condition inside the loop.	M	M	R	R
Verify testing to ensure that safety critical data items are protected from being overwritten by unauthorized operations.	M	M	M	M
Independent verification that all modules identified as safety critical are tested at the required level at least once.	M	M	M	M
Error case testing must be performed to test the handling of unexpected values. This must include analysis of all plausible errors that will be considered for the test.	M	M	M	R
Perform stress testing to verify limits of safety critical modules.	M	M	R	R
Verification of the ability of the software to handle large and out-of-range values.	M	M	R	R
Perform black box tests written specifically for safety critical functions.	M	M	R	R
Test to ensure that every safety critical thread through the code is followed and leads to a desired outcome.	M	M	R	R
Perform stress testing where inputs are varied to exceed the limits specified in the SRS and to force system anomaly conditions (e.g., division by zero). The goal is to discover where the software design and timing limits break down.	M	M	R	R
Test all modules and functions at least once.	M	M	M	M
For each new build, perform regression testing to verify subsequent builds do not impact the previously tested safety critical functionality. Also perform safety regression testing for software modifications or revisions within a build. Create a minimum set of unit, unit integration, and software qualification regression test cases for testing all safety critical software functionality.	M	M	R	R

Notes: *M – Mandatory task*
R – Recommended task
NR- Not Required task, however, normal CMMI-based processes apply
"Independence" implies independence from the Software Development Team.

This is an EXAMPLE of what can be included in an SIAM but it must be reiterated that the contents of this matrix are negotiated with the software development and test teams and approved by the PM. Further guidance of what can be included in the matrix is provided below in paragraph A.6.2.4.

A.6.2.4 Software Safety Integrity Requirements and Tasks

Some suggested software safety integrity tasks that can be applied to a program are listed in the following paragraphs for consideration and applicability.

A.6.2.4.1 Design Requirements

The following design requirements must be considered: fault tolerant design, fault detection, fault isolation, fault annunciation, fault recovery, warnings, cautions, advisories, redundancy, independence, N-version design, functional partitioning (modules), physical partitioning (processors), design safety guidelines, design safety standards, best and common practices.

A.6.2.4.2 Process Tasks

Consider the following process tasks: design review, safety review, design walkthrough, code walkthrough, independent design review, independent code review, independent safety review, traceability of SCFs, SCF code review, SCF design review, test case review, test procedure review, safety test result review, independent test results review, safety quality audit inspection, software quality assurance (SQA) audit, safety sign-off of reviews and documents.

A.6.2.4.3 Test Tasks

The following are test task considerations: SCF testing, functional thread testing, limited regression testing, 100% regression testing, failure modes and effects testing, safety critical interface testing, commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) input/output testing and verification, independent testing of prioritized SCFs, functional qualification testing, IV&V.

A.6.3 Software Safety Risk Assessment

After completion of all the specified software safety engineering and integrity tasks (including system qualification tests), results will be used as evidence (or input) to the residual safety risk associated with single hazard risk (r) and total system risk (R). Software safety engineering with the software development team (and possibly the independent verification team) must evaluate the results of all the safety verification activities and perform a qualitative assessment of confidence for each safety critical requirement. This information must be integrated into the safety assessment report or safety case.

A.7 Contract Terms and Conditions

Some acquisitions include the following conditions in their solicitation, system specification, or contract as requirements for the system design. These condition statements are used optionally as supplemental requirements based on specific program needs, and are worded below as they would appear if used in this manner.

A.7.1 Unacceptable Conditions

The following safety critical conditions are considered unacceptable for development efforts. Positive action and verified implementation is required to reduce the mishap risk associated with these situations to a level acceptable.

- Single component or multi-component single-point failure, common mode failure, human error, or a design feature that could result in a mishap of critical or catastrophic severity.
- Dual independent component failures, dual independent human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could result in a mishap of catastrophic severity.
- Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.
- Packaging or handling procedures and characteristics that could cause a mishap for which no mitigators have been provided to protect personnel or sensitive equipment.
- Hazard categories that are specified as unacceptable in the development agreement.
- Component design or location that fails to address human physical, anthropometrics, physiological and/or perceptual-cognitive capabilities or limitations.

A.7.2 Acceptable Conditions

The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once mitigating actions are implemented and verified to an acceptance condition.

- For non-safety critical command and control functions: a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.
- For safety critical command and control functions: a system design that requires at least three independent failures, or three independent human errors, or a combination of three independent failures and human errors.
- System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.
- System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.
- System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.
- System designs that provide an approved safety factor, or a fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.

- System designs that control energy build-up that could potentially cause a mishap (e.g., fuses, relief valves, or electrical explosion proofing).
- System designs where component failure can be temporarily tolerated because of residual strength or alternate operating paths, so that operations can continue with a reduced but acceptable safety margin. (When feasible, consider providing a warning indicator when a primary control system fails or the alternative control system is engaged).
- System designs that positively alert the controlling personnel to a hazardous situation where the capability for operator reaction can been provided.
- System designs that limit or control the use of hazardous materials.

A.8 Example – Safety Design Requirements

The chief engineer, and utilizing systems engineering and associated system safety professionals, must establish specific safety design requirements for the overall system. The objective of safety design requirements is, through the application of design guidance, to establish a baseline of mishap risk from which risk can be further reduced to ALARP using an effective system safety program. Design guidance includes standards, specifications, regulations, design handbooks, safety design checklists, and other sources. Review these for safety design parameters and acceptance criteria applicable to the system. Safety design requirements derived from the selected parameters, as well as any associated acceptance criteria, are included in the system specification. Expand these requirements and criteria for inclusion in the associated follow-on or lower level specifications. See general safety system design requirements below.

A.8.1 Hazardous Material

Hazardous material use is minimized, eliminated, or associated mishap risks are reduced through design, including material selection or substitution. When using potentially hazardous materials, select those materials that pose the least risk throughout the life cycle of the system.

A.8.2 Hazardous Material Isolation

Hazardous substances, components, and operations are isolated from other activities, areas, personnel, and incompatible materials.

A.8.3 Equipment Location

Equipment is located so that access during operations, servicing, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous substances, high voltage, electromagnetic radiation, and cutting and puncturing surfaces).

A.8.4 Safety Protection

Protect power sources, controls, and critical components of redundant subsystems by physical separation or shielding, or by other acceptable methods.

A.8.5 Safety Devices

Consider safety devices that will minimize mishap risk (e.g., interlocks, redundancy, fail safe design, system protection, fire suppression, and protective measures such as clothing, equipment, devices, and procedures) for hazards that cannot be eliminated. Make provisions for periodic functional checks of safety devices when applicable.

A.8.6 System Final Disposition

System final disposition is considered in the design. A system final disposition plan must be developed and implemented that addresses all areas of disposition (disposal, recycling, etc.).

A.8.7 Warning Signals

Implement warning signals to minimize the probability of incorrect personnel reaction to those signals, and standardize within like types of systems.

A.8.8 Warning and Cautionary Notes

Provide warning and cautionary notes in assembly, operation, and maintenance instructions; and provide distinctive markings on hazardous components, equipment, and facilities to ensure personnel and equipment protection when no alternate design approach can eliminate a hazard. Use standard warning and cautionary notations where multiple applications occur. Standardize

notations in accordance with commonly accepted commercial practice or, if none exists, normal military procedures. Do not use warning, caution, or other written advisory as the only risk reduction method for hazards that could result in a major mishap.

A.8.9 Personnel Proficiency

Safety critical tasks may require personnel proficiency; if so, the Developer must propose a proficiency certification process to be used.

A.8.10 Mishap Minimization

Severity of injury or damage to equipment or the environment as a result of a mishap is minimized.

A.8.11 Safety Requirements

Inadequate or overly restrictive requirements regarding safety are not included in the system specification.

A.8.12 Acceptable Risk

Acceptable risk is mishap risk that is ALARP within the constraints of operational effectiveness, time, and cost as determined by the appropriate authority. This level of mishap risk is achieved and maintained by implementing new technology, materials, or designs in a system's production, test, and operation. Changes to design, configuration, production, or mission requirements (including any resulting system modifications and upgrades, retrofits, insertions of new technologies or materials, or use of new production or test techniques) are accomplished in a manner that keep the level of mishap risk as low as reasonably practicable. Changes to the environment in which the system operates are analyzed to identify and mitigate the mishap risk of any new hazards or changes in the risk of known hazards.

Annex B — System Safety Tasks

B.1 General.

This appendix provides the tasks that can be selectively applied to fit a tailored System Safety Program. The sequence of task and subtask accomplishment must be tailored to the individual program to which they are being applied. The 100-series Tasks apply to safety program management and control. The 200-series Tasks apply to safety design and integration. The 300-series Tasks apply to safety design evaluation. The 400-series Tasks apply to safety compliance and verification.

B.2 Task Structure

Each individual task is divided into three parts: purpose, task description, and details to be specified.

a. The “PURPOSE” provides a brief reason for performing the task.
b. The “TASK DESCRIPTION” provides the actual subtasks that comprise the task that a contractor must perform if specified by the Managing authority. Task descriptions must be tailored by the Managing authority as required by governing regulations and as appropriate to particular systems or equipment, program type, magnitude, and funding. In tailoring the tasks, the detail and depth of the effort is defined by the Managing authority and incorporated in the appropriate contractual documents. When preparing proposals, the Developer may include additional tasks or task modifications with supporting rationale for each addition or modification.
c. The “DETAILS TO BE SPECIFIED” paragraph under each task description lists specific details, additions, modifications, deletions, or options to the requirements of the task that must be considered by the Managing authority when tailoring the task description to fit program needs. This information is then included in the document in which the task is invoked. The list provided with each task is not necessarily complete and may be supplemented by the Managing authority. "Details to be Specified" annotated by an "(R)" are required and must be provided to the Developer by the Managing authority for proper implementation of the task, if the task is to be contractually implemented.

Task 101 – System Safety Program

101.1 Purpose

The purpose of Task 101 is to establish the foundation for a system safety program. The total system safety program consists of this task plus any other tasks from Sections 100, 200, 300, 400, or other source designated by the Managing authority.

101.2 Task Description

101.2.1 Establish a System Safety Program

Establish and execute a system safety program which meets the tailored requirements of Section 4, General Requirements, and all other tasks/requirements designated by the Managing authority.

101.2.2 Develop a Planned Approach

Develop a planned approach for safety task accomplishment, provide qualified people to accomplish the tasks, establish the authority for implementing the safety tasks through all levels of management, and allocate appropriate resources, both manning and funding, to assure the safety tasks are completed.

101.2.3 Establish a System Safety Organization

Establish a system safety organization or function and lines of communication within the program organization and with associated organizations (Managing authority and Developer). Establish interfaces between system safety and other functional elements of the program, as well as between other safety disciplines such as nuclear, range, explosive, chemical, biological, etc. Designate the organizational unit responsible for executing each safety task. Establish the authority for resolution of identified hazards.

101.2.4 Define System Safety Program Milestones

Define system safety program milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs.

101.2.5 Establish a Reporting Process

Establish an incident alerting/notification, investigation and reporting process, to include notification of the Managing authority.

101.3 Details to be Specified

Details to be specified in the SOW must include the following, as applicable:

(R) a. Imposition of Task 101.
(R) b. Tailoring of Section 4 to meet specific program requirements.
(R) c. Acceptable level of risk with reporting thresholds.
(R) d. Minimum mishap probability and severity reporting thresholds.
e. MA requirements for incident processing.
f. Requirement for and methodology of reporting to the Managing authority the following:
(1) Mishap hazards/risks.
(2) Safety critical functions and safety features to mitigate risk.
(3) Operating, maintenance and overhaul safety requirements.
(4) Measures used to abate hazards.

(5) Acquisition management of hazardous materials.

g. Qualifications for key system safety personnel.

h. Other specific system safety program requirements.

Task 102 – System Safety Program Plan

102.1 Purpose

The purpose of Task 102 is to develop a System Safety Program Plan (SSPP). It must describe, in detail, the tasks and activities of system safety management and system safety engineering that are required to identify, evaluate, and eliminate or control hazards, or reduce the associated risk to as low as reasonably practicable as determined by the Managing authority throughout the system life-cycle. The approved plan provides a formal basis of understanding between the contractor and Managing authority on how the system safety program must be executed to meet contractual requirements, including general and specific provisions.

102.2 Task Description

The Developer must develop an SSPP to provide a basis of understanding between the Developer and the Managing authority as to how the system safety program must be accomplished to meet contractual safety requirements included in the general and special provisions of the contract. The approved plan must, on an item-by-item basis, account for all contractually required tasks and responsibilities. The SSPP must include the following:

102.2.1 Program Scope and Objectives

Each SSPP must describe, as a minimum, the four elements of an effective system safety program:
1) a planned approach for task accomplishment,
2) qualified people to accomplish tasks,
3) authority to implement tasks through all levels of management, and
4) appropriate commitment of resources (both manning and funding) to assure that tasks are completed.

The SSPP must define a program to satisfy the system safety requirements imposed by the contract. This section must:

a. Describe the scope of the overall program and the related system safety program.
b. List the tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks that are applicable to system safety and identify where they are specified or described.
c. Account for all contractually required safety tasks and responsibilities. A matrix must be provided to correlate the requirements of the contract to the location in the SSPP where the requirement is addressed.

102.2.2 System Safety Organization

The SSPP must describe:

a. The system safety organization or function within the organization of the total program using charts to show the organizational and functional relationships, and lines of communication. The organizational relationship between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization must be shown. Review and approval authority of applicable tasks by system safety must be described.

b. The responsibility and authority of system safety personnel, other contractor organizational elements involved in the system safety effort, subcontractors, and system safety groups. Describe the methods by which safety personnel may raise issues of concern directly to the PM or the PM's supervisor within the corporation. Identify the organizational unit responsible for executing each task. Identify the authority in regard to resolution of all identified hazards.
c. The staffing of the system safety organization for the duration of the contract to include manpower loading, control of resources and a summary of the qualifications of key system safety personnel assigned to the effort, including those who possess coordination and approval authority for Developer-prepared documentation.
d. The procedures by which the Developer must integrate and coordinate the system safety efforts including assignment of the system safety requirements to action organizations and subcontractors, coordination of subcontractor system safety programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.
e. The process through which Developer management decisions must be made including timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, program deviations, etc.
f. Details of how resolution and action relative to system safety will be affected at the program management level possessing resolution authority.

102.2.3 System Safety Program Milestones

The SSPP must:

a. Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.
b. Provide a program schedule of safety tasks including start and completion dates, reports, and reviews.
c. Identify subsystem, component, software safety activities as well as integrated system level activities (i.e., design analyses, tests, and demonstrations) applicable to the system safety program but specified in other engineering studies and development efforts to preclude duplication.
d. Provide the estimated manpower loading required to complete each task.

102.2.4 General System Safety Requirements and Criteria

The SSPP must:

a. Describe general engineering requirements and design criteria for safety. Describe safety requirements for support equipment and operational safety requirements for all appropriate phases of the life-cycle up to, and including, disposal. List the safety standards and system specifications containing safety requirements that must be complied by the contractor. Include titles, dates, and where applicable, paragraph numbers.
b. Describe the risk assessment procedures. The mishap severity categories, mishap probability levels, and the system safety precedence that must be followed to satisfy the safety requirements of the program. State any qualitative or quantitative measures of safety to be used for risk assessment including a description of the acceptable/unacceptable risk levels. Include system safety definitions which modify, deviate from or are in addition to those in this standard.

c. Describe closed-loop procedures for taking action to resolve identified unacceptable risk including those involving non-developmental items.

102.2.5 Hazard Analysis

The SSPP must describe:

a. The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met.

b. The depth within the system to which each technique is used including hazard identification associated with the system, subsystem, components, software, hazardous materials, personnel and human systems integration, ground support equipment, non-developmental items, facilities, and their interrelationship in the logistic support, training, maintenance, operational and disposal (including render safe and emergency disposal) environments.

c. The method of ensuring flow down of safety critical functions and associated requirements to the supplier and integration of subcontractor/supplier hazard analyses with overall system hazard analyses.

d. Efforts to identify and control hazards associated with materials used during the system's life-cycle.

e. The boundaries and key assumptions used for hazard analyses and the limits of the analyses. This typically includes:
   (1) Hostile intentions or sabotage upon the system are not examined.
   (2) Basic structural integrity is not analyzed.
   (3) Hazards unique to factory support are not analyzed.
   (4) It is assumed that only trained, healthy, working-age adults will operate and support the system.
   (5) Appropriate quality control and configuration standards are used in production, assembly and support.
   (6) The analysis will have a limit of resolution. The limit is dependent on the system and details of the hazard. It may change as more information on the system is acquired.

f. A systematic approach to:
   (1) Implementing the software system safety unique tasks, activities, and work products (software safety requirements analysis; top-level, detailed, design-level, code-level analyses, change analysis, and test analysis).
   (2) Identifying and describing the software hazards.
   (3) Identifying safety critical software functions and safety critical software requirements.
   (4) Identifying the Software Criticality Index (SCI) for each safety critical software function and its associated requirements.
   (5) Assigning safety critical functions and requirements.
   (6) Specifying verification method of yielding objective evidence of correct software implementation and functions.
   (7) Performing a final risk assessment for software related hazards.

102.2.6 System Safety Data

The SSPP must:

a. Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned data.
b. Identify deliverable data by title and number, and means of delivery (e.g., hard copy, electronically, etc.).
c. Identify non-deliverable system safety data and describe the procedures for accessibility by the Managing authority and retention of data of historical value.

102.2.7 Safety Verification

The SSPP must describe:

a. The verification (test, analysis, inspection, etc.) requirements and method for providing concrete evidence in artifacts and test results that safety is adequately demonstrated.
b. Procedures for making sure that safety-related verification information is transmitted to the Managing authority for review and analysis.
c. Procedures for ensuring that the mishap risk of the testing itself is as low as reasonably practicable.

102.2.8 Audit program

The SSPP must describe the techniques and procedures to be employed by the contractor to make sure that the objectives and requirements of the system safety program are being accomplished.

102.2.9 Training

The SSPP must describe the safety training for engineering, technician, operating, and maintenance personnel.

102.2.10 Incident Reporting

The contractor must describe, in the SSPP, the mishap/incident alerting/notification, investigation, and reporting process including notification of the Managing authority.

102.2.11 System Safety Interfaces

The SSPP must identify, in detail:

a. The interface between system safety and all other applicable safety disciplines.
b. The interface between system safety, systems engineering, and all other support disciplines such as: maintainability, quality control, reliability, software development, human system integration, medical support (health hazard assessments), and any others.
c. The interface between system safety and all system integration and test disciplines.

102.2.12 Contractor-Supplied Plan

The contractor must provide a plan that complies with the requirements in paragraph 102.2 in their reply to the solicitation as part of their proposal or integrated master plan and must be made a part of the contract.

102.3 Details to be Specified

Details to be specified in the solicitation must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 102.
b. Identification of additional information to be provided.

Task 103 – Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms

103.1 Purpose

The purpose of Task 103 is to provide the Developer and Managing authority with appropriate management surveillance of the system safety program, and the capability to establish and maintain uniform integrated system safety program requirements. This task must also describe requirements for associate contractors, subcontractors, and architect and engineering firms' (AE) system safety programs. This task can also be used to require the flow down of system safety requirements to subcontractors, suppliers, and vendors.

103.2 Task Description

103.2.1 Integrator

The integrator for the safety functions of all associate/sub contractors must:

a. Prepare an integrated system safety program plan (ISSPP) as the SSPP required by Task 102 defining the role of the integrator and the effort required from each associate contractor to help integrate system safety requirements for the total system. In addition to the other contractually imposed requirements, the plan must address and identify:
   (1) Definition of where the control, authority and responsibility transitions are from Developer to associates and subcontractors.
   (2) Analyses, risk assessment, and verification data to be developed by each associate contractor with format and method to be utilized.
   (3) Data each associate/sub contractor is required to submit to the integrator and its scheduled delivery, keyed to program milestones.
   (4) Schedule and other information considered pertinent by the integrator.
   (5) The method of development of system level (including software) requirements to be allocated to each of the associate subcontractors as a part of the system specification, end-item specifications, and other interface requirement documentation.
   (6) Safety-related data pertaining to non-developmental items (NDI).
   (7) Integrated safety analyses to be conducted and support required from associate and subcontractors.
   (8) Developer roles in test range, nuclear safety, explosive, or other certification processes.

b. Initiate action, through the Managing authority, to make sure that each associate contractor is required to be responsive to the ISSPP. Recommend contractual modification where the need exists.

c. When conducting risk assessments, analyze the integrated system design, operations, and, specifically, the interfaces between the products of each associate contractor or subcontractor and the end item. Data or analyses provided by associate contractors and subcontractors must be used in the conduct of this effort.

d. When performing a safety assessment, summarize the mishap risk presented by the operation of the integrated system. Data or analyses provided by associate contractors or subcontractors must be used in the conduct of this effort.

e. Provide assistance and guidance to associate contractors regarding safety matters.

f. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to system and item specifications. Where problems cannot be resolved by the integrator, notify the Managing authority for resolution and action.
g. Initiate action through the Managing authority to make sure that information required by an associate/subcontractor (from the integrating contractor or other associate contractors) to accomplish safety tasks, is provided in an agreed-to format.
h. Develop a method of exchanging safety information between associate/subcontractors. If necessary, schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort. Use of System Safety Group/System Safety Working Group (SSG/SSWG) meetings must be included as required.
i. Implement an audit program to make sure that the objectives and requirements of the system safety program are being accomplished. Whenever the Developer believes an associate contractor has failed to meet contract requirements, the Developer must notify the Managing authority in writing. The integrator for the safety effort must send a copy of the notification to the associate contractor.

103.2.2 Associate Contractor

Associate contractors must provide safety data and support (including participation in SSGs/SSWGs) needed by other associate contractors and the Developer to the extent specified in the contract.

103.2.3 Subcontractors

Applicable provisions of this standard must be included in all contracts with major subcontractors. The “chain of responsibility” for formally flowing down the system safety contractual requirements from the Developer to different levels of subcontractors, suppliers, and vendors (who provide different applicable subsystems, equipment and/or parts) must be identified.

a. All subcontractors are required to maintain suitable documentation of safety analyses they have performed in formats that will permit incorporation of their data into the overall analysis program.
b. Major subcontractors are required to develop system safety program plans to be included as annexes to the prime contractor’s SSPP.
c. Lesser subcontractors and vendors are required to provide information on software, component and subassembly characteristics, including failure modes, failure rates, and possible hazards, which will permit Developer prime contractor personnel to evaluate the items for their impact on safety of the system.
d. All subcontractors must participate in the SSG and SSWGs, when required.

103.2.4 Architect and Engineering Firms

The AE must be responsible for conducting facility hazard analyses and other facility SSPP functions as specified in the solicitation. The AE must be responsible for securing the expertise necessary to perform the required work and must have the same responsibilities as a prime contractor in hazard identification, tracking, and resolution. The AE must assure that design subcontractors or consultants maintain and provide suitable documentation of any safety analyses performed.

103.3 Details to be Specified

Details to be specified in the solicitation must include the following, as applicable:

(R) a. Imposition of Tasks 101, 102 and 103 as tailored.
(R) b. Designation of the system safety contractor (Developer).
c. Designation of status of the other associate/subcontractors.
d. Requirements for any special integrated safety analyses.
e. Requirements to support test range, nuclear safety, explosive, environmental or other certification processes.
f. Description of specific integration roles.

Task 104 – System Safety Program Reviews/Audits

104.1 Purpose

The purpose of Task 104 is to establish a requirement for the Developer to perform and document system safety program reviews/audits or support of reviews/audits performed by the Managing authority. This task is also used to acquire support for special requirements such as certifications and test/flight readiness reviews.

104.2 Task Description

104.2.1 Perform and Document System Safety Program Reviews/Audits

The Developer must perform and document system safety program reviews/audits as specified by the Managing authority. These reviews/audits must be performed on:

a. The Developer's system safety program.
b. The associate contractors' system safety programs.
c. The support contractors' system safety programs.
d. The subcontractors' system safety programs.

104.2.2 Support System Safety Reviews/Audits

The Developer must support system safety reviews/audits performed by representatives of the Managing authority to the extent specified in the contract.

104.2.3 Support Certifying Presentations

To the extent specified by the Managing authority in the contract, the Developer must support presentations certifying activities such as phase safety reviews, munitions safety boards, nuclear safety boards, or flight safety review boards. These may also include special reviews such as flight/article readiness reviews or preconstruction briefings.

104.3 Details to be Specified

Details to be specified in the contract must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 104.
(R) b. Identification of reviews/audits, their content, and probable locations.
c. Method of documenting the results of system safety reviews/audits.
d. Frequency of system safety reviews/audits.

Task 105 – System Safety Group/System Safety Working Group Support

105.1 Purpose

The purpose of Task 105 is to require Developers to support System Safety Groups (SSGs) and System Safety Working Groups (SSWGs), which are established in accordance with service regulations or as otherwise defined by the Managing authority.

105.2 Task Description

The Developer must participate as an active member of Managing authority SSG/SSWGs. Such participation must include activities specified by the Managing authority such as:

a. Presenting the Developer safety program status, including results of design or operations risk assessments.
b. Summarizing hazard analyses, including identification of problems, status of resolution, and mishap risk.
c. Presenting incident assessments (especially mishaps and malfunctions of the system being acquired) results including recommendations and action taken to prevent recurrences.
d. Responding to action items assigned by the chairman of the SSG/SSWG.
e. Developing and validating system safety requirements and criteria applicable to the program.
f. Identifying safety deficiencies of the program and providing recommendations for corrective actions or preventions of reoccurrence.
g. Planning and coordinating support for a required certification process.
h. Documenting and distributing meeting agendas and minutes when required by the Managing authority.

105.2.1 Subcontractors

The Developer shall require that all major subcontractors participate in the SSG/SSWGs.

105.2.2 Associate Contractor

The Developer shall require that all associate contractors participate in the SSG/SSWGs.

105.3 Details to be Specified

Details to be specified in the solicitation must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 105.
(R) b. Developer membership requirements and role assignments, e.g., recorder, member, alternate, or technical advisor.
(R) c. Frequency or total number of SSG/SSWG meetings and probable locations.
(R) d. Requirement for the contractor to prepare and distribute the agenda and minutes of the SSG/SSWG.
e. Specific SSG/SSWG or other presentation support tasks.

Task 106 – Hazard Tracking and Risk Resolution

106.1 Purpose

The purpose of Task 106 is to establish a single, closed-loop, hazard tracking system.

106.2 Task Description

106.2.1 Documents

The Developer must develop a method or procedure to document and track hazards and their controls thus providing an audit trail of hazard resolutions. A centralized file, computer data base, or document called a “Hazard Log” must be maintained. The Hazard Log must contain as a minimum:

a. Description of each hazard, to include associated mishap risk.
b. Status of each hazard and control.
c. Traceability of resolution on each Hazard Log item from the time the hazard was identified to the time the risk associated with the hazard was reduced to a level acceptable to the Managing authority.
d. Identification of mishap risk.
e. Action persons and organizational element.
f. The recommended controls to reduce the hazard to a level of risk acceptable to the Managing authority.
g. The signature of the Managing authority accepting the risk and thus effecting closure of the Hazard Log item.

106.2.2 Data

The contractor must deliver a copy of the Hazard Log to the Managing authority as required in the list of contract deliverables.

106.3 Details to be Specified

Details to be specified in the solicitation must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 106.
(R) b. Procedure by, and detail to, which hazards are entered into the log.
(R) c. Procedure by which the contractor must obtain close-out or risk acceptance by the Managing authority of each hazard.
d. Complete set of data required on the hazard log, including format.
e. Identification of any special requirements involving a computerized log.

Task 107 – System Safety Progress Summary

107.1 Purpose

The purpose of Task 107 is to prepare a periodic progress report summarizing the pertinent system safety management and engineering activity that occurred during the reporting period.

107.2 Task Description

107.2.1 Periodic System Safety Progress Report

The Developer must prepare a periodic system safety progress report summarizing general progress made relative to the system safety program during the specified reporting period, and projected work for the next reporting period.

107.2.2 Data

The Developer must prepare a report in Developer format that contains the following information:

a. A brief summary of activities, progress, and status of the safety effort in relation to the scheduled program milestones. It must highlight significant achievements and problems. It must include progress toward completion of safety data prepared or in work.
b. Newly recognized significant hazards and significant changes in the degree of control of the risk of known hazards.
c. Individual hazard resolution status and status of all recommended corrective actions that have not been implemented.
d. Significant cost and schedule changes that impact the safety program.
e. Discussion of contractor documentation reviewed by the system safety function during the reporting period. Indicate whether the documents were acceptable for content and whether inputs to improve the safety posture were made.
f. Proposed agenda items for the next system safety group/working group meeting, if such groups are formed.

107.3 Details to be Specified

Details to be specified in the contract must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 107.
(R) b. Specification of progress reporting period.

Task 108 – Launch Safety Program Requirements

108.1 Purpose

The purpose of this task is to require the Developer to support special safety requirements specific to launch facilities and range design and operation.

108.2 Task Description

The Developer must comply with the following requirements (as tailored by the Managing authority) when this task is called out in the contract.

108.2.1 Unacceptable/Acceptable Conditions

a. Unacceptable conditions. The following safety critical conditions are considered unacceptable. Positive action and implementation verification is required to reduce the risk to an acceptable level as negotiated by the Developer and the Managing authority.
   (1) Single component failure, common mode failure, human error, or design features that could result in a mishap as defined by the Managing authority.
   (2) 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 result in a mishap as defined by the Managing authority.
   (3) 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.
   (4) Packaging or handling procedures and characteristics that could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.
   (5) Hazard level categories that are specified as unacceptable in the contract.

b. Acceptable conditions. The following approaches are considered acceptable for correcting unacceptable conditions and will require no further analysis once controlling actions are implemented and verified.
   (1) For non safety critical command and control functions; a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.
   (2) For safety critical command and control functions; a system design that requires at least three independent failures, or three human errors, or a combination of three independent failures and human errors.
   (3) System designs that positively prevent errors in assembly, installation, or connections that could result in a mishap.
   (4) System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.
   (5) System design limitations on operation, interaction, or sequencing that preclude occurrence of a mishap.
   (6) System designs that provide an approved safety factor or fixed design allowance that limits, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.
   (7) System designs that control energy build-up that could potentially cause a mishap (fuses, relief valves, electrical explosion proofing, etc.).

(8) System designs in which component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin.
(9) System designs that positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been provided.
(10) System designs that limit/control the use of hazardous materials.

108.2.2 Associate Safety Programs.

108.2.2.1 Industrial Safety and Hygiene

The Developer must conduct the system safety program so that it augments and supplements existing industrial safety and toxicology activities. This coordinated effort must assure that equipment or properties being used or developed under contract are protected from damage or mishap risk. When Developer owned or leased equipment is being used in manufacturing, testing, or handling of products developed or produced under contract, analysis and operational proof checks must be performed to show that risk of damage to those products has been minimized through proper design maintenance and operation by qualified personnel using approved procedures. This standard does not cover those functions that the Developer is required by law to perform under Federal or State OSHA, DOT, or EPA regulations.

108.2.2.2 Operational Site Safety

The Developer system safety program must encompass operational site activities. These activities must include all operations listed in the operational time lines, including system installation, checkout, modification, and operation. Particular attention must be given to operations and interfaces with ground support equipment and to the needs of the operators relating to personnel subsystems such as: panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.

108.2.2.3 Facilities

The Developer must include facilities in the system safety analyses activity. Facility safety design criteria must be incorporated in the facility specification. Consideration must be given to the test, operational, and maintenance aspects of the program. Identified requirements must include consideration of the compatibility with standards equal to or better than those specified by the most stringent of Federal, State, and Local Regulations. The test and operations safety procedures must encompass all development, qualification, acceptance tests, and operations. The procedures must include inputs from the safety analyses and must identify test, operations, facility, and support requirements. The procedures must be upgraded and refined as required to correct deficiencies identified by the system safety analyses to incorporate additional safety requirements.

108.2.3 Range Safety

Compliance with the design and operational criteria contained in the applicable range safety manuals, regulations, and standards must be considered in the system safety analysis and the system safety criteria. System safety is concerned with minimizing risk to on- or off-site personnel and property arising from system operations on a range.

108.2.4 Drone and Missile System Safety

a. Verification of system design and operational planning compliance with range or operating site safety requirements must be documented in the SAR or as otherwise specified in the contract SOW and CDRL.
b. Ensure that flight analysis and flight termination systems comply with the requirements of the test range being utilized. Such requirements are applicable to the system during all flight phases until vehicle/payload impact or orbital insertion. The SAR or other safety report, as specified in the CDRL, must include all aspects of flight safety systems.
c. The Developer's system safety representatives will be an integral part of the flight evaluation and assessment team that reviews field/flight operations to correct any identified deficiencies and recommend appropriate safety enhancements during the field/flight operation process.

108.3 Details to be Specified

Details to be specified in the contract must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 108.
(R) b. Identification of the paragraphs in Task 108 that apply or do not apply.

Task 109 – Test Hazard Analysis Safety (Ground or Airborne Systems)

109.1 Purpose

The purpose of Task 109 is to establish a requirement for the Developer to assess and document hazards associated unique to test safety activities.

109.2 Task Description

109.2.1 Ground and/or Flight Test Safety Program

An effective ground and/or flight test safety program must be implemented any time support of unqualified systems or air vehicles (manned or unmanned) are to be ground/flight tested with residual risk, spiral software, regression testing, or other test operations.

109.2.2 Test Hazard Analyses

Test hazard analyses must be performed to determine ground or flight risk, and to recommend mitigation and any restrictions, aircraft operating limitations, temporary operating procedures, special precautions, or emergency procedures.

109.2.3 Independent Aircraft Test Safety Review Boards

Independent aircraft test safety review boards must be convened as required to assess overall safety risk of the hardware, software, system, human system integration, airworthiness, mitigations, flight clearances, and other areas as required.

109.3 Details to be Specified

Details to be specified in the contract must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 109.

(R) b. Identification of the paragraphs in task 109 that apply or do not apply.

Task 201 – Preliminary Hazard List (PHL)

201.1 Purpose

The purpose of Task 201 is to compile a list of potential hazards, very early in the system development cycle, on which management emphasis needs to be placed.

201.2 Task Description

The contractor must:

201.2.1 Compile a PHL

Examine the system shortly after the concept definition effort begins and compile a list (PHL) identifying possible hazards that may be inherent in the concept and their associated mishap potential, or identify hazards specified by the Managing authority.

201.2.2 Review Safety Experience

Review safety experience on similar systems, including mishap/incident hazard tracking logs (if accessible), safety lessons learned, etc., to identify possible hazards and their mishap risks. The sources of a hazard found in this review must be referenced in the PHL.

201.2.3 Investigate Hazards Identified in the PHL

Further investigate selected hazards or hazardous characteristics identified in the PHL as directed by the Managing authority to determine their significance.

201.2.4 Data

The Developer must prepare a Report that contains the results from the work task described by paragraph 201.2 above to include the following information:

201.2.4.1 Hazard Analysis Results

This must consist of a summary or a total listing of the results of hazard analysis. Contents and formats must be as agreed upon between the Developer and the Managing authority. The following are the content requirements unless otherwise modified:

a. A summary of the results.
b. A listing of identified potential hazards, in narrative or matrix (sometimes called columnar or tabular) format, to include the following information:
   (1) Hazard Description.
      (a) A brief description of the hazard in terms that identify a source, mechanism, and an outcome, for example, "Radiation leakage from radar set waveguide harming nearby personnel."
      (b) The recommended action required to eliminate or control the hazard.
      (c) Any information relating to the hazard not covered in other blocks; for example, applicable documents, previous failure data on similar systems, or administrative directions.

201.3 Details to be Specified

Details to be specified in the SOW must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 201.
b. Identification of special concerns, hazards, or undesired events that the Managing authority wants listed or investigated.

Task 202 – Preliminary Hazard Analysis

202.1 Purpose

The purpose of Task 202 is to perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions.

202.2 Task Description

202.2.1 Perform and Document a Preliminary Hazard Analysis

The Developer must perform and document a preliminary hazard analysis to obtain an initial risk assessment of a concept or system. Based on the best available data, including mishap data (if assessable) from similar systems and other lessons learned, hazards associated with the proposed design or function must be evaluated for mishap severity, mishap probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to the Managing authority must be included. The PHA must consider the following for identification and evaluation of hazards as a minimum:

a. Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).
b. Safety related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This must include consideration of the potential contribution by software (including software developed by other contractors/sources) to subsystem/system mishaps. Safety design criteria to control safety critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or Managing authority-designated undesired events) must be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.
c. Operating conditions including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation).
d. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage). Those test unique hazards that will be a direct result of the test and evaluation of the article or vehicle.
e. Facilities, real property installed equipment, support equipment (e.g., provisions for storage, assembly, checkout, or proof testing of hazardous systems/assemblies that may involve toxic, flammable, explosive, corrosive, or cryogenic materials/wastes; radiation or noise emitters; electrical power sources), and training (e.g., training and certification pertaining to safety operations and maintenance).
f. Safety related equipment, safeguards, and possible alternate approaches (e.g., interlocks; system redundancy; fail safe design considerations using hardware or software controls;

subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).

g. System, subsystem, or software malfunctions must be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.

202.2.2 Report Requirements

The Developer must prepare a Report that contains the results from the work task described by paragraph 202.2 above to include the following information:

202.2.2.1 System Description

This must consist of summary descriptions of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation, must be supplied when such documentation is available. The capabilities, limitations, and interdependence of these components must be expressed in terms relevant to safety. The system, and its components, must be addressed in relation to its mission and its operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. Software and its roles must be included in this description.

202.2.2.2 Data

This must consist of summaries of data used to determine the safety aspects of design features.

202.2.2.3 Hazard Analysis Results

This must consist of a summary or a total listing of the results of hazard analysis. Contents and formats may vary according to the individual requirements of the program. The following are the content and format requirements for Hazard Analysis Results:

a. A summary of the results.

b. A listing of identified hazards, in narrative or matrix (sometimes called columnar or tabular) format, to include the following information:

(1) System/Subsystem/Unit. Enter the particular part of the system that this analysis is concerned with. For example, if this items applies to a radar system modulator, enter "modulator." If there are several modulators in the system, be sure to clearly specify which one the analysis pertains to.

(2) System Events Phase. The configuration or phase of the mission that the system is in when the hazard is encountered; for example, during maintenance, during flight, during pre-flight, full-power applied, etc. Tha hazard could be encountered in multiple or all system events.

(3) Hazard Description. A brief description of the hazard in terms that identify a source, a mechanism, and an outcome, for example, "Radiation leakage from radar set waveguide harming nearby personnel."

(4) Effect of Hazard. The detrimental effects that could be inflicted on the subsystem, system, other equipment, facilities or personnel, by this hazard. Possible upstream and downstream effects must also be described.

(5) Risk Assessment. A risk assessment for each hazard (classification of severity and probability of occurrence). This is the assessment of the risk prior to taking any action to eliminate or control the hazard.

(6) Recommended Action. The recommended action required to eliminate or control the hazard. Sufficient technical detail is required in order to permit the design engineers to adequately develop and assess design criteria resulting from the analysis. Include alternative designs and life-cycle cost impact where appropriate.

(7) Effect of Recommended Action. The effect of the recommended action on the assigned risk assessment. This is the risk assessment after taking action to eliminate or control each hazard. If the recommended action will result in cost/schedule/performance penalties to the extent that the Developer requires Managing authority approval prior to incorporation, then these considerations must be addressed.

(8) Remarks. Any information relating to the hazard not covered in other blocks; for example, applicable documents, previous failure data on similar systems, or administrative directions.

(9) Status. The status of actions to implement the recommended, or other, hazard controls. The status must include not only an indication of "open" or "closed," but also reference to the drawings, specifications, procedures, etc., that support closure of the particular hazard.

202.3 Details to be Specified

Details to be specified in the SOW must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 202.

(R) b. Minimum mishap probability and severity reporting thresholds.

c. Any selected hazards, hazardous areas, or other specific items to be examined or excluded.

Task 203 – Safety Requirements/Criteria Analysis

203.1 Purpose

The purpose of Task 203 is to perform and document the safety design requirements/design criteria for a facility or system under development/design.

203.2 Task Description

The Safety Requirements/Criteria Analysis (SRCA) relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level. The SRCA uses the Preliminary Hazard List (Task 201) or the Preliminary Hazard Analysis (Task 202) as a basis, if available. The SRCA is also used to incorporate design requirements that are safety related but not tied to a specific hazard. The analysis includes the following efforts:

203.2.1 Generic System Safety Design Requirements

The Developer must determine applicable generic system safety design requirements and guidelines for facilities; hardware, and software from federal, military, national, and industry regulations, codes, standards, specifications; and other documents for the system under development. The Developer must incorporate these requirements and guidelines into the high level system specifications and design documents as appropriate.

203.2.2 System Design Requirements Analysis

The Developer must analyze the System Design Requirements, System/Segment Specifications (SSS), Preliminary Hardware Configuration Item Development Specification, Software Requirements Specifications (SRS), and the Interface Requirements Specifications (IRS), or equivalent documents as appropriate, to include the following sub-tasks:

a. The Developer must 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 guidelines where appropriate; and implemented in the design and development of the system hardware and associated software.
b. The Developer must identify hazards and relate them to the specifications or documents listed above and develop design requirements to reduce the risk of those hazards.
c. The Developer must identify safety critical computer software components (SCCSCs) and ensure they are placed under configuration control. Safety critical software functions and requirements must be identified, traced, analyzed, tested, and verified at the appropriate levels (system integration, top level, detail design, unit level, code).
d. The Developer must analyze the preliminary system design to identify potential hardware/software interfaces at a gross level that may control, cause or contribute to potential hazards. Interfaces identified must include control functions, monitoring functions, safety systems and functions that may have indirect impact on safety. These interfaces and the associated software must be designated as safety critical.
e. The Developer must perform a preliminary mishap risk assessment on the identified safety critical software functional requirements using the mishap risk matrix or software hazard criticality matrix of Appendix A or another process as mutually agreed to by the Developer and the Managing authority.
f. The Developer must ensure that System Safety design requirements are properly incorporated into the operator, user, and diagnostic manuals.

203.2.3 Safety Related Design Change Recommendations and Testing Requirements

The Developer must develop safety related design change recommendations and testing requirements and must incorporate them into Preliminary Design Documents and the hardware, software and system test plans. The following sub-tasks must be accomplished:

a. The Developer must develop safety-related change recommendations to the design and specification documents listed above and must include a means of verification for each design requirement.
b. The Developer must develop safety related test requirements for incorporation into the test documents. Tests must be developed for hardware, software and system integration testing.

203.2.4 Developer Support

The Developer must support the System Requirements Review (SRR), System Design Review (SDR) and Software Specification Review (SSR) from a system safety viewpoint. The Developer must address the system safety program, analyses performed and to be performed, significant hazards identified, hazard resolutions or proposed resolutions, and means of verification.

203.2.5 Report Requirements

The Developer must prepare a report that contains the results from the work task described by paragraph 203.2 above to include the following:

203.2.5.1 System Description

This must consist of summary descriptions of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation, must be supplied when such documentation is available. The capabilities, limitations and interdependence of these components must be expressed in terms relevant to safety. The system and components must be addressed in relation to its mission and its operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. Software and its roles must be included in this description.

203.2.5.1.1 Generic System Safety Design Requirements and Guidelines

A list of the applicable generic system safety design requirements and guidelines for facilities; hardware and software from federal, military, national and industry regulations, codes, standards, specifications; and other documents for the system under development that have been determined to be applicable.

203.2.5.1.2 Data

This must consist of summaries of data used to determine the safety aspects of design features.

203.2.5.1.3 Hazard Analysis Results

This must consist of a summary or a total listing of the results of hazard analysis. Contents and formats may vary according to the individual requirements of the program. The following are the content and format requirements for Hazard Analysis Results:

a. A summary of the results.

b. Recommended action. The recommended action required to eliminate or control the hazard. Sufficient technical detail is required in order to permit the design engineers to adequately develop and assess design criteria resulting from the analysis. Include alternative designs and life-cycle cost impact where appropriate.

203.3 Details to be Specified

Details to be specified in the SOW must include the following, as applicable:

(R) a. Imposition of Tasks 101 and 203 tailored to the developmental program.
(R) b. Definition of acceptable level of risk within the context of the system, subsystem, or component under analysis.
(R) c. Level of Developer support required for design reviews.
d. Specification of the types of risk assessment process.

Task 204 – Subsystem Hazard Analysis

204.1 Purpose

The purpose of Task 204 is to perform and document a Subsystem Hazard Analysis (SSHA) to: verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents; identify previously unidentified hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem; recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels.

204.2 Task Description

The Developer must perform and document a subsystem hazard analysis to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements. This must include furnished equipment, non-developmental items, and software. Areas to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. The human must be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct of this analysis.

204.2.1 Required Elements

The analysis must include a determination:

a. Of the modes of failure including reasonable human errors as well as single point and common mode failures, and the effects on safety when failures occur in subsystem components.
b. Of potential contribution of hardware and software (including that which is developed by other developers/sources) events, faults, and occurrences (such as improper timing) on the safety of the subsystem.
c. That the safety design criteria in the hardware, software, and facilities specifications have been satisfied.
d. That the method of implementation of hardware, software, and facilities design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has it introduced any new hazards or risks.
e. Of the implementation of safety design requirements from top level specifications to detailed design specifications for the subsystem. The implementation of safety design requirements developed as part of the PHA and SRCA must be analyzed to ensure that it satisfies the intent of the requirements.
f. Of test plan and procedure recommendations to integrated safety testing into the hardware and software test programs.
g. That system level hazards attributed to the subsystem are analyzed and that adequate control of the potential hazard is implemented in the design.

204.2.2 Managing Authority Approval

If no specific analysis techniques are directed or if Developer recommends that a different technique than specified by the Managing authority must be used, the Developer must obtain Managing authority approval of techniques to be used prior to performing the analysis.

204.2.3 Software Development

When software to be used in conjunction with the subsystem is being developed under other development documents; the developer/subcontractor performing the SSHA must monitor, obtain and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA. Problems identified that require the reaction of the software developer must be reported to the Managing authority in time to support the ongoing phase of the software development process.

204.2.4 Required Updates

The Developer must update the SSHA as a result of any system design changes, including software design changes, that affect system safety.

204.2.5 Report Requirements

The Developer must prepare a report that contains the results from the work task described by paragraph 204.2 above to include the following information:

204.2.5.1 System Description

This must consist of summary descriptions of the physical and functional characteristics of the system and its components. Reference to more detailed system and component descriptions, including specifications and detailed review documentation must be supplied when such documentation is available. The capabilities, limitations and interdependence of these components must be expressed in terms relevant to safety. The system and components must be addressed in relation to its mission and its operational environment. System block diagrams or functional flow diagrams may be used to clarify system descriptions. Software and its roles must be included in this description.

204.2.5.2 Data

This must consist of summaries of data used to determine the safety aspects of design features.

204.2.5.3 Hazard Analysis Results

This must consist of a summary or a total listing of the results of hazard analysis. Contents and formats may vary according to the individual requirements of the program. The following are the content and format requirements for Hazard Analysis Results:

a. A summary of the results.
b. A listing of identified hazards, in narrative or matrix (sometimes called columnar or tabular) format, to include the following information:
   (1) Components Failure Modes. All component failure modes that can result in a hazard. Failure modes generally answer the question of “how” it fails.
   (2) System Events Phase. The configuration or phase of the mission that the system is in when the hazard is encountered; for example, during maintenance, during flight, during pre-flight, full-power applied, etc., or it could be encountered in all system events.
   (3) Description. A complete description of the potential/actual hazards inherent in the item being analyzed, or resulting from normal actions or equipment failure, or handling of hazardous materials.
   (4) Effect of Hazard. The detrimental effects which could be inflicted on the subsystem, system, other equipment, facilities or personnel, resulting from this hazard. Possible upstream and downstream effects must also be described.