

***Space and Missile Systems Center
SMCI 63-1205
Air Force Space Command
United States Air Force***

20 August 2007


SPACE SYSTEM SAFETY POLICY, PROCESS, AND TECHNIQUES

**OPR: SMC/SES (Dr Louis Huang)
Certified by: SMC/SE (Mr. Phillip Rodriguez)**

Pages: 76

This instruction applies to all Space and Missile Center (SMC) developed, operated and acquired space and missile systems and ground support equipment. It shall be continuously used and periodically updated in conjunction with other Operational Safety, Suitability and Effectiveness OSS&E instructions. This document implements Air Force Policy Directive AFPD 63-12 and Air Force Instruction AFI 63-1201, "Assurance of Operational Safety, Suitability, & Effectiveness" for space and missile systems, and addresses portions of AFI 10-1211, "Space Launch Operations." This document helps synchronize the requirements of Space Missile Center Instruction SMCI 63-1202, "Space Flight Worthiness", SMCI 63-1203 "Independent Readiness Review Team", and SMCI 63-1204 "SMC Readiness Review Process" by sequencing them to the contractual acquisition phases. This document provides instruction in utilizing the principles within National Security Space NSS-03-01, the space and system safety objectives outlined in AFI 91-202 "Air Force Mishap Prevention Program", and MIL-STD 882C "System Safety Program Requirements" (as directed by the SMC Director of Safety).

APPROVED:


PHILLIP RODRIGUEZ, GG-15
Director of Safety, SMC
Los Angeles AFB

APPROVED:



JAMES R. HOREJSI, Col
Chief Engineer, SMC
Los Angeles AFB

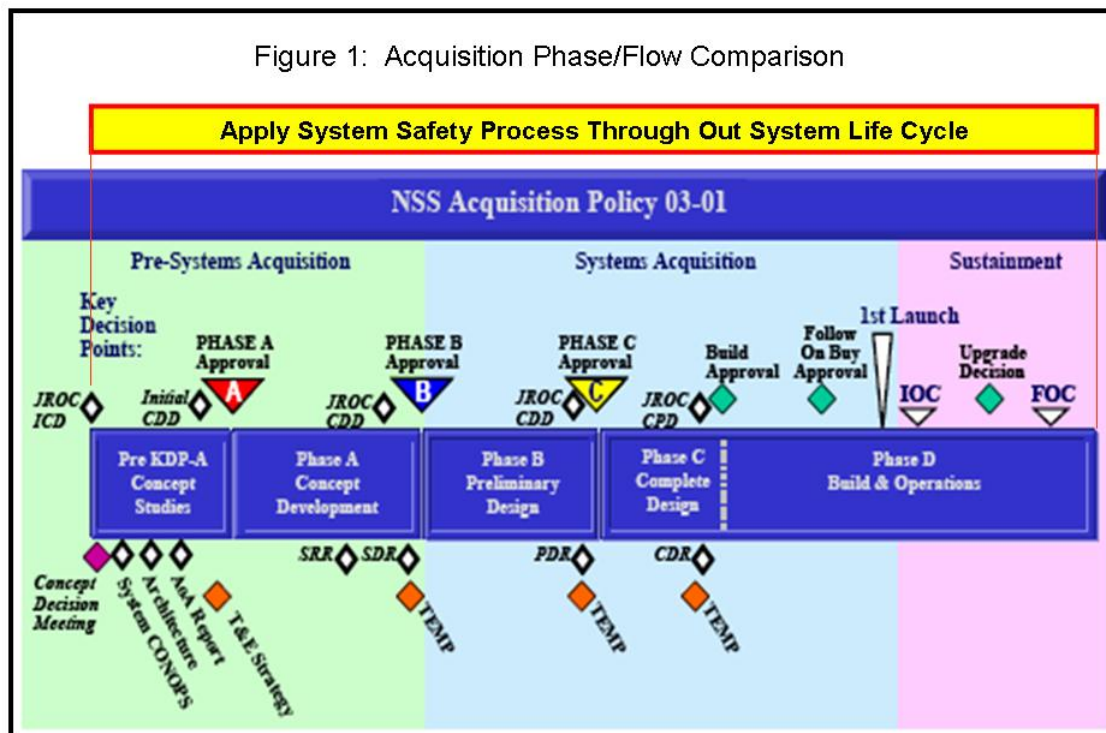
TABLE OF CONTENTS

TABLE OF CONTENTS	2
1.0 Introduction.....	4
1.1 Contribution to Mission Success.....	4
1.2 Relationship to Other Technical Functions.....	5
2.0 System Safety Concepts.....	5
2.1 Definition of Terms.....	5
2.2 System Safety Order of Precedence	8
2.3 Mishap Risk Conditions	9
2.4 Risk Assessment and Management	10
3.0 System Safety Process in the SMC Program Lifecycle.....	10
3.1 Concept Studies (Pre-Phase A)	11
3.1.1 System Safety during Concept Studies	11
3.2 Concept Development Phase (Phase A)	13
3.2.1 System Safety during Concept Development Phase	13
3.3 Preliminary Design (Phase B)	14
3.3.1 System Safety during Preliminary Design	14
3.4 Complete Design (Phase C)	15
3.4.1 System Safety during Complete Design	16
3.5 Build and Operations (Phase D)	17
3.5.1 System Safety during Build and First Launch	17
3.5.2 Orbital Operations and Safety.....	18
3.5.3 System Safety during Sustainment.....	19
3.6 End-of-Life Disposal Implementation.....	20
4.0 System Safety Functions.....	20
4.1 System Safety Management	20
4.1.1 The System Safety Manager Roles and Responsibilities	21
4.1.2 MIL-STD-882C Tailoring and Associated CDRLs and DIDs	23
4.1.3 Request for Proposal Instructions to Bidders (RFP Section L).....	28
4.1.4 Request for Proposal Evaluation Criteria and Standards (RFP Section M)	29
4.1.5 Work Breakdown Structure (WBS).....	30
4.1.6 The System Safety Management Plan and Task Planning.....	30
4.1.7 Risk Ranking, Tracking, and Residual Risk Acceptance.....	31
4.1.8 Meetings	32
4.1.9 System Safety Information Architecture and Maintenance	34
4.2 System Safety Engineering.....	36
4.2.1 System Safety Engineering's Role in Systems Engineering	36
4.2.2 Hazard Analysis and its Techniques	38
4.2.3 Mishap Risk Mitigation and Control	48
4.2.4 Mishap Risk Verification	49
4.3 System Safety in Operations and Testing	50
4.3.1 Test System Safety	51
4.3.2 Operational and Space System Safety.....	52
4.3.3 Operational and Space Safety Tasks.....	52

4.3.4	Corrective Actions	52
4.3.5	Qualified People	52
4.3.5	Establishing authority	53
4.3.6	Resources	53
5.0	System Safety Relationship to Other Activities.....	53
5.1	Programmatic Environmental Safety and Health Evaluation.....	53
5.2	Operational Safety, Suitability, and Effectiveness.....	54
5.4	Range Safety	54
5.5	Operational Risk Management.....	55
Appendix A: Major System Safety Products.....		57
A. 1	System Safety Management Plan	57
A.2	Sample Language for Statement of Objectives	60
A.3	Sample Language for Statement of Work	60
A.4	Preliminary Hazard Analysis Table.....	61
A.5	Hazard Control Report	62
A.6	Hazard Risk Acceptance	63
A.7	Example Tailored MIL-STD-882C Task Lists.....	66
A.7.1	Example Tailored MIL-STD-882C Task List: Satellite/Launch Vehicle	66
A.7.2	Example Tailored MIL-STD-882C Task List: Ground System	68
A.8	Contractor Data Requirements Lists (CDRLs)	69
A.9	Data Item Descriptions (DID) List and Accessible Data Products List (ADPL)	70
A.10	DIDs and MIL-STD-882C Tasks Matrix.....	71
Appendix B: Acronyms		72
Appendix C: Applicable Documents		76
Appendix D: Bibliography and Recommended Reading		76

1.0 Introduction

Program Managers, regardless of the Acquisition Category of their programs, are required to integrate system safety into their overall systems engineering and risk management processes (USD AT&L Letter, Sep 23 2004). This document describes the System Safety Process at SMC that implements the AFI 91-202, AFSPCMAN 91-710 and MIL-STD 882C. It shall be used in conjunction with the Operational Safety, Suitability and Effectiveness (OSS&E) Instruction (AFI 63-1201) and the National Security Space Acquisition Policy (NSS 03-01). Figure 1 is a model acquisition flow. It is intended for application through the life cycle of each space and missile acquisition program (i.e., launch vehicles, spacecraft, ground, and user equipment acquisition programs). It covers the development of a solicitation, contract award, and management of the acquired system(s), from initial concept through the end of the program life, including disposal.



1.1 Contribution to Mission Success

Through its systematic identification and control of the System Program Office's (SPO's)¹ mishap risks, the system safety engineering process provides critical support to

¹ Due to the wide variety of organizations at SMC, for the purposes of this document, the expressions "System Program Office", "Joint Program Office", "System Wing", and "System Group" may be used interchangeably; they all essentially denote the top-level of management for the program. Similarly, the executive in charge of the program office may be referred to as the "System Program Director" (SPD),

the program's ability to meet its performance, cost and schedule goals. If this process is not implemented, or is not thoroughly planned and effectively applied, the resulting impact to the program may be catastrophic. These mishap-related risks include loss of mission, personnel injuries, equipment damage, environmental contamination, or ultimately the degradation or failure of the mission and/or loss of human life.

The execution of the system safety process produces a major portion of the required documentation used to meet the SMC mandated Space Flight Worthiness (SFW) criteria. SMC/EA and SMC/SE collectively create and maintain, with approval from the SMC Commander, the criteria for Space Flight Worthiness.

1.2 Relationship to Other Technical Functions

The system safety engineering process interfaces with the other entire set of engineering disciplines as part of the SPO's total risk management process. Consideration of the mishap risk is an integral part of each engineering design task, each technical trade off study/decision, each test plan/test execution and operating procedure.

Each SPO will gain benefit from the aggregated experience of the SMC Safety Office by requesting their support/attendance in SPO processes and at SPO events. The SPO Director shall provide to the SMC Safety Office (SMC/SE) access to SPO and contractor personnel, documentation, meetings and facilities to facilitate its support. In turn, SMC/SE shall provide system safety expertise to help define and resolve SPO system safety issues.

2.0 System Safety Concepts

System safety is implemented through common management and engineering operations throughout the life cycle of the program, from concept through disposal. System safety is a program specific engineering process. System Safety studies are conducted to identify and mitigate or minimize negative impacts to personnel, the system and the environment in accordance with regulatory requirements, cost, schedule, design and operational constraints. The degree of safety achieved in a given system is directly dependent upon the amount of government and contractor emphasis.

2.1 Definition of Terms

Hazard – A condition with the potential to cause harm.

Hazard Report (HR) – A report used for tracking and mitigating hazards. This report contains the details of the hazard, how it affects the system, the risks, and all necessary

“System Program Director”, “Program Manager” (PM), “System Wing Commander”, or “System Group Commander”.

references needed to track the hazard. This report also contains the signatures of the persons responsible for accepting the hazard.

Hazard Risk Assessment Matrix (HRAM) – A matrix that shows each hazard, its probability, and level of severity. This matrix is very useful in quickly assessing the overall program risks. It is sometimes referred to as a *Hazard Action Matrix* or *Mishap Risk Assessment Matrix*.

High Accident Potential (HAP) Events - Significant aircraft, missile, space, explosives, miscellaneous air operations, or ground events with a high potential for causing injury, occupational illness, or damage if they recur. These events do not have reportable mishap costs.

As defined in AFI 91-202, “USAF Mishap Prevention Program”, Space incidents/anomalies that do not meet the Class A, B, C or D mishap or Class E event reporting criteria, but the cause of which could have important mishap prevention value, shall be investigated and reported as a HAP event. In this context, it is important for each incident to be investigated to determine the “root cause” and to extract information that could be useful in the exchange of mishap prevention information as “lessons learned”.

Mishap – An unplanned event, or series of events, that results in damage to DoD property; occupational illness to DoD military or civilian personnel; injury to DoD military personnel on/off duty; injury to on-duty civilian personnel; damage to public and private property or injury and illness to non-DoD personnel caused by DoD operations. Also includes the degradation of nuclear or radiological safety. Mishaps are further classified as follows:

Missile Mishap – Unplanned damage to or functioning of a missile; or damage, illness, or injury caused by a missile; or when the missile fails to complete its intended mission.

Orbital Mishap – For satellites, declaration of a space mishap will be based upon the permanent loss or degradation of a primary or non-primary mission capability. Degradation includes shortened life span and/or degraded data or mission performance.

Space Mishap – An accident involving a space system and/or unique space support equipment. Mishaps which occur prior to launch, or are limited to components or equipment commonly used in non-space applications, and not specifically configured for space related use will be classified as ground and industrial mishaps with space involvement.

Mission Capability – This term encompasses the purpose and functions of the space system throughout its intended system mean mission duration (e.g. the design life of the space vehicle).

Preliminary Hazard Analyses (PHA) – A basic hazard analysis, which establishes the framework for other hazard analyses and safety engineering evaluation of the design. It is designed to obtain an initial safety risk assessment of a concept or system. It is performed to identify safety critical areas, evaluate hazardous conditions and identify safety design criteria. The analysis results are used to develop safety requirements and to prepare performance, design and verification requirements.

Preliminary Hazard List (PHL) – A list of hazards developed at the very start of a program, or project to assess the suspected risks/hazards/mitigations. This list is only an assessment to focus the systems safety effort and is usually developed after the first review of the system description.

System Safety – System Safety is a process that applies engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle. System safety is also a value of a program or an attribute of a system similar to quality, reliability, or life cycle cost. System safety as an attribute is inversely related to mishap risk, and the process is sometimes called mishap risk management.

System Safety Engineer (SSE) - The SSE is a uniquely trained engineer who performs system safety engineering activities on behalf of the System Safety Manager.

System Safety Engineering - System Safety Engineering is an engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk.

System Safety Management - System safety management is the use of processes that plan, organize and control the program's mishap risk, as well as interfacing with other disciplines and organizations. Government and contractor management is responsible for providing a program with the necessary skilled personnel and resources to focus on the specific objectives of providing a product that is safe and meets all performance, cost and schedule requirements. The evolution of a comprehensive System Safety Program (SSP) is critical in the process of defining and integrating cost, schedule and performance requirements.

System Safety Manager (SSM) - The SSM is a uniquely trained engineer who performs system safety management activities on behalf of program management. The government or contractor SSM is officially assigned in writing by the appropriate program manager, system program director or materiel wing director. A SSM serving part time, assisting the primary SSM or in a geographically separate location is sometimes referred to as a System Safety Officer (SSO), and shall meet the same qualification requirements. There shall be at least one responsible full time System Safety Manager or System Safety Engineer per Systems Program Office, Joint Program Office or System Wing.

System Safety Management Plan (SSMP) - The SSMP is a document that contains guidance on how the System Program Office (SPO) or Joint Program Office (JPO) will implement System Safety requirements. When signed by both the SPO and SMC/SE, it ensures the planning, implementation, and accomplishment of system safety tasks and activities consistent with the overall program requirements. The SSMP is written for an overall government organization's effort, meeting the same types of requirements as an System Safety Program Plan (see below), and integrating, but not duplicating, associated documents such as contractor System Safety Program Plans.

System Safety Program Plan (SSPP) – When implemented as part of a tailored MIL-STD-882C, the SSPP is a description of the planned tasks and activities to be used by the responsible organization(s) to implement the required system safety program. This description includes organizational responsibilities, resources of funds and personnel, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

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

System - System is a composite, at any level of complexity, of personnel, procedures, material, tools, equipment, facilities, and software. 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 capability, purpose, support, or mission requirement.

2.2 System Safety Order of Precedence

In selecting specific hazard controls System safety engineers are generally guided by the following “System Safety Order of Precedence”. The order in which hazard controls shall be selected is as follows:

- ***Design for minimum risk*** – From the first design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level through design selection;
- ***Incorporate safety designs*** – If an identified hazard cannot be eliminated or its associated risk adequately reduced to an acceptable level through design selection, that risk shall be reduced to an acceptable level through the use of fixed, automatic or other protective safety design features or devices;
- ***Provide warning devices*** – When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce the associated risk, devices shall be used to detect the condition and to produce an adequate warning signal. Warning devices shall be designed to minimize false alarms and shall be standardized within similar systems;
- ***Develop procedures and training*** – Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety or

warning devices, procedures and training shall be used. However, without a specific waiver, no warning, caution or other form of written advisory shall be used as the only risk reduction. Procedures may include the use of personal protective equipment. Safety critical tasks may require the certification of personnel proficiency.

2.3 Mishap Risk Conditions

The following unacceptable and acceptable mishap risk conditions definitions are traditional and are appropriate for space systems. The words below are also available for use as contract and technical requirements through MIL-STD-882C.

Unacceptable conditions - The following safety critical conditions are considered unacceptable:

- Single component failure, common mode failure, human error, or design features which could cause a mishap of catastrophic or critical severity;
- Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of catastrophic or critical severity;
- 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;
- Packaging or handling procedures and characteristics which could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment;
- Hazard level categories that are specified as unacceptable in the contract.

Positive action and implementation verification is required to reduce the risk due to unacceptable conditions to an acceptable level.

Acceptable conditions - The following approaches are considered acceptable for correcting unacceptable conditions and require no further analysis once controlling actions are implemented and verified.

- 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 human errors, or a combination of three independent failures and human errors;
- System designs which positively prevent errors in assembly, installation, or conditions which could result in a mishap;
- System designs which 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 which preclude occurrence of a mishap;

- System designs that provide an approved safety factor, or fixed design allowance which limit, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap;
- System designs that control energy build-up which could potentially cause a mishap (Fuzes, relief valves, electrical explosion proofing, etc.);
- 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;
- System designs which positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been provided;
- System designs which limit/control the use of hazardous materials.

2.4 Risk Assessment and Management

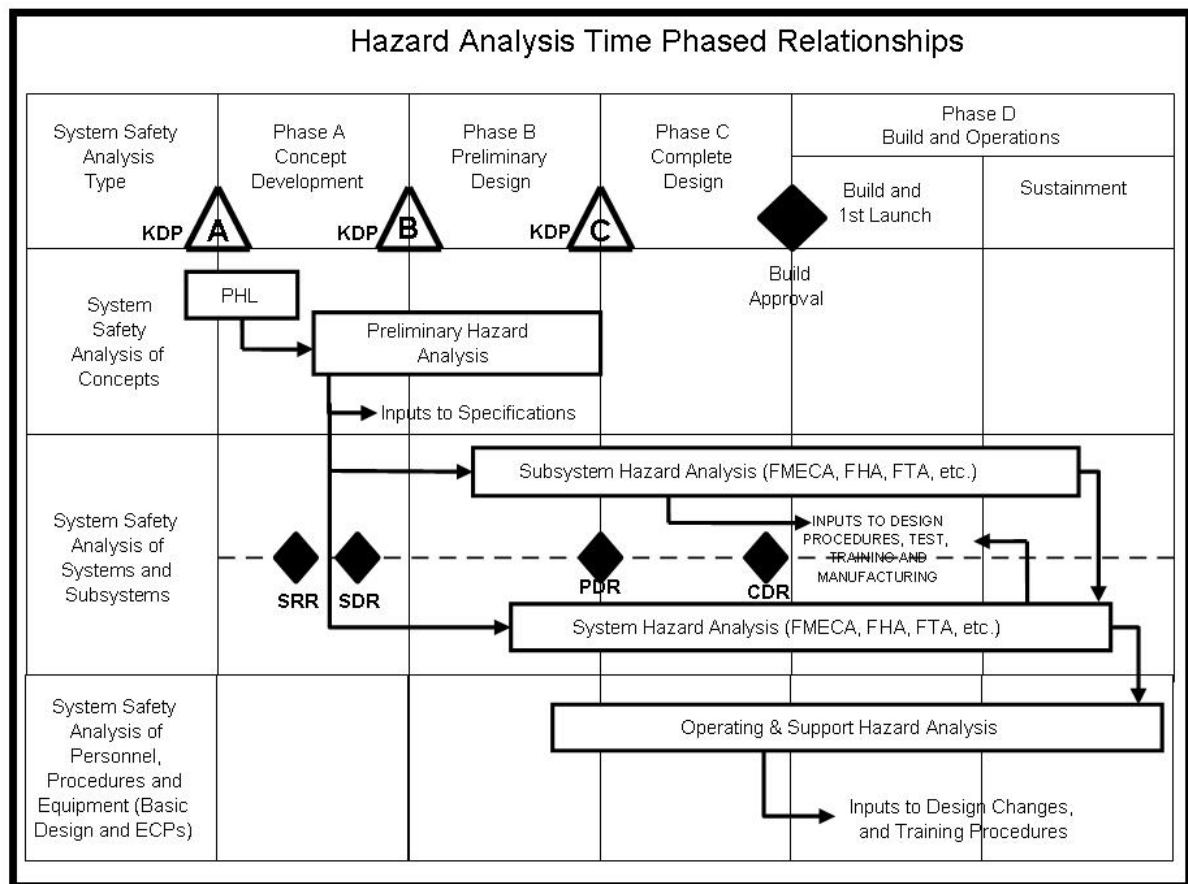
Under the current SMC Operational Risk Management (ORM) Integration and Sustainment Plan, System Safety and OSS&E are identified as integral parts of a program's risk management effort. The scope of the assurance and preservation of OSS&E covers a significant portion of all of the program's risk. The use of ORM-based system safety principles, tools, and techniques by all program office personnel are critical to assuring acceptable levels of risk throughout the life of the space or missile system. A SPO Risk Management Plan which defines the tasks to be performed by the government shall be in place to assess the impacts of all program risks. SMC programs are required to use system safety processes and tools to sustain baseline capabilities during all modifications, upgrades, block changes, training, and other activities.

The process must contain metrics that document how well the process is being employed in the measurement of the system's space flight worthiness.

3.0 System Safety Process in the SMC Program Lifecycle

Part of the System Safety engineering process is to participate in the pre-contract activities such as preparing request for proposal objectives and source selection criteria as well as post-award surveillance of the events depicted in the Integrated Master Plan/Integrated Master Schedule (IMP AND IMS) and the SSMP/SSPP.

The figure below illustrates the time-phased relationship of system safety analyses.



3.1 Concept Studies (Pre-Phase A)

During Concept Studies, activities such as development of the Initial Capabilities Document, Analysis of Alternatives, Systems-Level Concept of Operations, the Acquisition Strategy, and the Test and Evaluation Strategy are conducted by the concept sponsor. The goal of Concept Studies is to provide sufficient information for entry into the acquisition process.

3.1.1 System Safety during Concept Studies

The Government System Safety Manager or System Safety Engineer (SSM/SSE) will be intimately involved with the System Safety process as implemented by the Government/Contractor Team. The team assists in the evaluation of the various candidate architectures by providing essential information (energetic materials/explosives, hazardous materials, preliminary orbital debris analysis) to support the selection of the most suitable technical approach. A partial list of government SSM/SSE pre-Phase A activities and products are as follows:

- Request assistance from SMC/SES staff system safety engineers;

- Review and provide input to the ICD, System CONOPS, Analysis of Alternatives Report and Test and Evaluation Strategy;
- Help develop the acquisition strategy using the SMC/SES template;
- Provide input to the RFP, SOO, PESHE requirements and SSMP;
- Ensure that charters are written for the System Safety Group, the System Safety Working Group, and the PESHE Working Group;
- Participate in developing key documents including the Technical Requirements Document (TRD) and specifications, Independent Program Assessment checklists, Inspector General (IG) checklists, and SSM Continuity Folder;
- Develop criteria for proposal review/evaluation and participate in source selection;
- SSMs, program managers and contracting officers shall request a preliminary System Safety Program Plan as part of the proposal;
- Develop the draft preliminary hazard list;
- With SMC Staff support, develop a preliminary tailoring of MIL-STD 882C for the RFP;
- Develop draft probability and severity level definitions;
- Generate a draft Government System Safety Management Plan

The Contractor SSM/SSE provides inputs to the proposal, which includes, but may not be limited to, the contractor's initial System Safety Program Plan, the contractor Hazardous Material Management Program Plan (HMMPP), the Integrated Master Plan (IMP), Integrated Master Schedule (IMS), and Work Breakdown Structure (WBS). The contractor's SSPP and HMMPP shall provide for government participation in activities to include, but not be limited to IPTs, Configuration Control Board (CCBs), Technical Interchange Meeting (TIMs), SSG meetings, and SSWG meetings. The Contractor SSM/SSE will perform the required analyses and prepare reports for submittal during the contract period of performance. The following list lists some, but not all, of the contractor's SSM/SSE pre-Phase A activities and products:

- Write the preliminary contractor System Safety Program Plan (SSPP) and Hazardous Material Management Plan (HMMP) using the contractor's updated system description;
- Provide input to the IMP, and IMS;
- Define in the proposal the WBS elements that cover the contractor's system safety tasks;
- Define in the proposal how the contractor system safety program will interoperate with the government system safety process and database (Hazard Log).

The Government SSM/SSEs shall oversee the Contractor's activities and ensure that all system safety requirements are satisfied. The Government SSM/SSE shall:

- Review and approve the contractor's system safety program;
- Provide timely risk assessments to the appropriate government program manager to support the risk acceptance decisions.

The System Safety Program Plan and the System Safety Management Plan are required to be implemented throughout all phases of the program's life cycle. They map the system safety process to program phases to identify system safety activities, risks, issues, and regulatory requirements. They are used to minimize the impact to the program of hazards/risks and non-compliances.

3.2 Concept Development Phase (Phase A)

The Concept Development phase includes concept studies, assessments and requirements (e.g., technology development, Capability Development Document). During this phase, baseline development is mature enough to enter the formal acquisition process.

3.2.1 System Safety during Concept Development Phase

During Concept Development the System Safety process assists in the evaluation of the various candidate architectures and development of the selected concept by providing essential information (such as identification of energetic materials,/explosives, identification of hazardous conditions/operations) to support the selection of the most robust- mishap tolerant solution. Program specific System Safety requirements are validated and the program allocates resources to satisfy requirements.

The Contractor's system safety effort supports the Government's system safety effort by providing a preliminary hazard analysis, a hazard risk assessment matrix and an updated system safety program plan meeting MIL-STD-882C requirements for the proposed concept architecture. This support helps ensure the execution of the Government system safety management program with consistent and traceable system requirements.

Early participation and involvement in the system safety process by the Government staff (SPO, SMC Staff system safety organization/personnel) is required. The government SSM/SSE shall monitor the system safety program and ensure that unmitigated safety risks are brought to the attention of the system program director and program manager (SPD/PM) for review and resolution. During this period, the range safety function shall review the proposed design to ensure the proposed systems adhere to range safety requirements.

System Safety activities during the Concept Development Phase include:

- Appointment in writing of qualified System Safety Managers (both SPO and Contractor) and identification of system safety personnel;
- Establishment by the SPO of tools required to perform formal tracking of hazards, their closures, and identification/acceptance of residual mishap risk, to include a defined and documented risk acceptance authority for the life cycle of the program;
- Updating and implementing the government SSMP and the contractor SSPP;
- Creation of a System Safety Group Charter, to include scheduling of System Safety Group and System Safety Working Group Meeting(s);

- Incorporation by the SPO of system safety requirements/tasks into key documents such as the ASP, SOO, RFP, (C)SOW, CDD, and PESHE;
- Establishing criteria and evaluate contractor performance;
- Participation in requirements development, trade studies, and design reviews (i.e., the SRR and SDR);
- Review and validation by SPO System Safety of Contractor performed identification and analysis of hazards (PHL/PHA/HRAM);
- Planning for system disposal (both for on-orbit and ground based systems), demilitarization, and end-of-life requirements;
- Evaluation of system safety design features (hazard controls);
- Identify required safety tests and data;
- Identify safety requirements in test plans and procedures;
- Prepare reports, and data needed to support the milestone and OSS&E reviews;
- Further detail the system safety tasks (SSMP/SSPP) for later phases;
- Help begin the PESHE Working Group if not done, and prepare initial PESHE documentation;
- Develop and conduct program specific system safety training;
- Establishment by the SPO of a System Safety Program
- Ensure that system safety personnel have participated in all trade studies;

Development by the SPO System Safety manager of requirements to be contracted for the delivery of necessary data, and documentation for, system and range safety compliance (such as the MSPSP, PFDP, FFDP, MRAR, SAR, etc.)

3.3 Preliminary Design (Phase B)

The Preliminary Design phase increases confidence in system alternative(s) by assessing risk levels and projected performance at a detailed engineering level. Activities include efforts to mature technology and baseline management and definitization, which will culminate in a Preliminary Design Review.

3.3.1 System Safety during Preliminary Design

During Preliminary Design, the system safety process includes conducting analyses of systems, subsystems, components, production methods, system operations, and system maintenance. Prototyping of critical hardware items, software items and/or processes may be performed. Program unique system safety risks are identified and mitigations are implemented to eliminate or reduce the severity of the risks. Other unsafe conditions or actions, including possible regulatory violations, are identified and mitigated. The same range safety concerns and involvement during Concept Development are continued in this phase. The combined government/contractor system safety activities include:

- Update the government SSMP and the contractor SSPP;
- Verify that all system safety personnel are qualified to perform their duties;
- Conduct the System Safety Group (meet, set policy, assign detailed tasks, accept risks, etc.);

- Update and document system safety requirements (such as system safety specific, explosive safety, bioenvironmental, PESHE, space safety including range and orbital etc.);
- Complete a Preliminary Hazard Analysis including government review and input before PDR;
- Begin performing Subsystem Hazard Analyses using updated system description;
- Begin performing System Hazard Analyses using updated system description;
- Ensure participation by system safety personnel in requirements reviews, design reviews (such as the PDR) and other milestones;
- Begin performing Operating & Support Hazard Analyses using updated system description;
- Perform Hazardous Materials/Explosives Classification using updated system description;
- Begin performing Interface Safety Hazard Analyses using updated system description;
- Review and provide System Safety inputs to the CDD;
- Perform Hazard Analyses on test system plans, procedures, equipment and facilities using updated system description;
- Schedule required safety tests and data;
- Prepare for and support applicable Test Safety Reviews;
- Perform Hazard Analysis on disposal of SPO generated space debris and ground residue;
- Generate Hazard Reports (HRs) from the safety hazard analyses;
- Develop and document hazard mitigations and verifications (special tests, trade studies, etc.);
- Update planned next phase system safety effort (e.g. contractors' procedures for storage, handling, packaging of hazardous materials);
- Prepare summary reports for milestones and OSS&E briefs;
- Utilization by the SPO of their approved tracking tool for the tracking of hazards, their closures, and identification/acceptance of residual mishap risk;
- Ensure that the SPO fund system safety-related tasks in the RFP and/or the (C)SOW
- Conduct program specific system safety training;
- Review and validation by SPO System Safety of Contractor performed identification and analysis of hazards (updated PHA, SSHA, and SHA);
- Preparation and coordination by the SPO of initial MSPSP, PFDP, FFDP, MRAR, SAR, etc., packages to verify compliance with system and range safety requirements;
- Update by the SPO of documentation on system disposal, orbital debris mitigation, and end-of –life requirements
- Update by SPO of system safety requirements in all test plans and procedures;
- Input by SPO System Safety into the Capability Production Document.

3.4 Complete Design (Phase C)

The Complete Design phase includes a baseline design and support concept of sufficient detail to support the Critical Design Review and Capability Production Document development.

3.4.1 System Safety during Complete Design

During Complete Design, system safety efforts are concentrated on the evaluation of the selected system designs to assure conformance with space system safety requirements, as well as verifying that manufacturing processes will be successful in producing a safe and affordable product.

In this Phase, activities remaining after Preliminary Design are continued at a deeper level of detail. Additionally the subsystem, system and operating support hazard analyses contain more fidelity.

System safety compliance information and study results are provided to government decision makers for use in the build and operations decision process. Refine and finalize the integrated SSP, the SSPP and the PESHE. Government/contractor activities and products include:

- Implement SSPP/PESHE;
- Update and document system safety requirements (e.g., system safety, energetic materials, bioenvironmental and range safety);
- Participate in requirements reviews, design reviews, trade studies, and other milestones;
- Review manuals, tech orders, emergency procedures for hazards;
- Refine test requirements to ensure verification of design;
- Evaluate mishaps/failures, perform tradeoff studies and define mitigations;
- Verify safety/protective equipment, safety training and handling procedures;
- Set disposal (on-orbit and ground based) and demilitarization requirements;
- Review contractors' procedures for storage, handling, packaging for safety impacts;
- Review and validation by SPO System Safety of contractor performed identification and analysis of hazards (SSHA and SHA), using updated system description;
- Ensure design incorporated system safety critical requirements (review drawings/specs);
- Mitigate the hazards identified in Phase C and previous phases;
- Review logistics support for safety consideration (software change and part replacement);
- Prepare appropriate report(s) for milestone and OSS&E reviews;
- Update the government SSMP and the contractor SSPP;
- Conduct System Safety Group meetings (set policy, assign detailed tasks, accept risks, etc.)

- Update and document system safety requirements (such as system safety specific, explosive safety, bioenvironmental, PESHE, space safety including range and orbital etc.);
- Participate in requirements reviews, design reviews and other milestones;
- Perform Hazardous Materials/Explosives Classification using updated system description;
- Perform Hazard Analyses on test system plans, procedures, equipment and facilities using updated system description;
- Schedule required safety tests and data;
- Prepare for and support applicable Test Safety Review Boards (TSRBs);
- Continue generating Hazard Reports (HRs) and other documentation from the safety hazard analyses;
- Develop and document hazard mitigations and verifications (special tests, trade studies, etc.);
- Update planned next phase system safety effort (e.g. contractors' procedures for storage, handling and packaging of hazardous materials);
- Prepare summary reports and presentations for milestones (CDR), key decisions (build approval), independent reviews, and OSS&E briefs;
- Maintain the database of risks and mitigations;
- Preparation and coordination by the SPO of initial MSPSP, PFDP, FFDP, MRAR, SAR, etc., packages to verify compliance with system and range safety requirements;
- Conduct program specific system safety training.

3.5 Build and Operations (Phase D)

The Build and Operations phase includes system-level fabrication, integration, testing, deployment, and operational support. Phase D can be further subdivided into two sub-Phases: Build and First Launch, and Sustainment.

3.5.1 System Safety during Build and First Launch

During the Build and First Launch, system safety efforts are concentrated on the evaluation of the selected system designs to assure conformance with contractual system safety requirements, as well as verifying that manufacturing processes will be successful in producing a safe and affordable product. System safety compliance information and study results are provided to government decision makers for use in the full-scale production decision process. Maintain and update the SSMP, SSPP, PESHE, and the safety database (mishap risk database and hazard log). Government/contractor activities include:

- Update the government SSMP and the contractor SSPP;
- Conduct System Safety Group activities and meeting(s);
- Participate in requirements and/or design reviews;

- Review manuals, tech orders, operating instructions, emergency procedures for hazards;
- Provide hazard controls, safety procedures and steps for operations and documents;
- Conduct tests to ensure verification of safe design;
- Evaluate mishaps/anomalies, perform tradeoff studies and define mitigations;
- Verify safety/protective equipment, safety training and handling procedures;
- Conduct Test Safety Review Board (TSRB);
- Implement requirements for disposal (on-orbit and ground based) and demilitarization;
- Review contractors' procedures for storage, handling and packaging for safety impacts;
- Perform hazard analyses (SHA/O&SHA) using updated system description;
- Ensure design incorporated system safety critical requirements (review drawings/specs);
- Mitigate the hazards identified in Phase D and previous phases;
- Review logistics support for safety considerations (software change and part replacement);
- Prepare appropriate data, report(s) and presentations for milestone events and reviews (LRR, MRR, FRR);
- Maintain the database of risks and mitigations;
- Conduct program specific system safety training.

3.5.2 Orbital Operations and Safety

Orbital safety, in accordance with AFI 91-202 AFSPC Sup, Chapter 11, covers activities, after orbital insertion, associated with testing and operating space vehicles in orbit or deep space, including reentry, recovery and disposal. Orbital safety begins in the earliest phases of a program when it must be incorporated in the design phase.

Orbital safety should cover, at a minimum:

- Collision Avoidance (minimize the risk of on-orbit collisions with other satellites or space debris, maintaining separation of functional and non-functional space objects through coordinated launch window management, accurate tracking and orbital element set updating; and coordination of planned orbit changes and evasive maneuvering to preserve operational space systems and to avoid the generation of additional space debris);
- Directed Energy (appropriate action to minimize hazards or interference with spacecraft or the general public and property on the earth's surface or in the atmosphere) , Orbital Debris Minimization(minimize the generation of orbital debris during and after their service life);
- Orbital vehicle end-of-life safing (the spacecraft should safely reenter the atmosphere or be moved into a disposal orbit at the end of its useful life where it will be less likely to interfere with operational spacecraft);

- Space Environment (designed to minimize damage due to natural phenomena such as meteoroids, solar radiation, spacecraft charging and high energy cosmic radiation, solar flares, etc.).

As part of the orbital safety effort, an on-orbit hazard analysis describing possible hazards to the spacecraft during on-orbit operations shall be generated by the contractor prior to the PDR, and updated by the CDR.

Programs that fail to have contractors conduct such on-orbit hazard analysis are still responsible for the satisfaction of this requirement; failure to do so must be noted as a Program Risk by the Program Manager, for either resolution or acceptance by the Program Executive.

3.5.3 System Safety during Sustainment

During the Sustainment Sub-phase, hazards, mitigations or controls are identified, documented and reviewed to determine if the system will meet system safety policy, regulation and plans during all tests and operations. Unresolved safety issues are brought to the appropriate government management level for final resolution.

During this period, system safety actions are also concentrated on manufacturing operations and maintenance activities to ensure consistency with system safety requirements. System safety management support is required during sustainment, decommissioning and disposal. System safety activities conducted during this period include:

- Update SSMP/SSPP tailored for production/deployment;
- Conduct System Safety Group Meeting(s);
- Update PESHE;
- Update and document system safety requirements (O&SHA and disposal of space debris/ground residue);
- Attend selected meetings (ops, design, test, etc.) to monitor system safety;
- Evaluate system/design changes that impact safety and recommend mitigations;
- Evaluate substitution of critical parts that impact safety and recommend mitigations;
- Evaluate operations and maintenance pubs that impact safety and recommend mitigation;
- Evaluate mishaps, Class E events, HAPs and anomalies: recommend mitigations;
- Help provide system safety lessons learned for other programs and systems;
- Review plans/procedures for control and disposal of hazardous materials;
- Review proposed production line changes for impact to system safety;
- Review test and evaluation activity for impact to the systems safety;
- Review procedures for storage, handling and packaging for safety impacts;
- Evaluate and report the status of all safety mitigation actions;
- Review all test plans for safety impacts;

- Prepare reports for milestones and reviews;
- Maintain the database of risks and mitigations;
- Conduct program and subsystem/system specific system safety training

3.6 End-of-Life Disposal Implementation

At the end of its useful life, a system shall be demilitarized and disposed in accordance with the legal and regulatory requirements and policy relating to safety (including space/orbital, systems, and explosive safety), security, and the environment. During the design process, Program Managers shall document hazardous materials contained in the system and shall estimate and plan for the system's demilitarization and safe disposal

During the end-of-life disposal, both ground and space based hazard mitigations or controls shall be implemented to meet existing safety plans and requirements. Residual risk acceptance decisions will be identified and brought to the attention of the appropriate government risk acceptance individual.

4.0 System Safety Functions

Section 3 discussed the involvement of the system safety process throughout the lifecycle of a system. In this section the system safety tasks are organized into three functional groupings:

Management - tasks primarily involved with organization and personnel, risk management, and task planning, scheduling, authorization, and monitoring.

Engineering – tasks involved in hazard identification and analysis, mishap risk mitigation, and mishap risk verification.

Operations and Testing – system safety tasks involved in operations and testing include the test safety review board process, space flight worthiness criteria, and corrective actions.

4.1 System Safety Management

System Safety is the responsibility of the Program Manager. The Government SSM manages the system safety effort on his behalf, and as such is considered a “direct report” to the Program Manager while performing this function. The System Program Director/Manager shall appoint his SSM in writing, with the concurrence of the SMC Director of Safety, and a copy of the appointment letter shall be provided to SMC/SE for archival purposes.

The system safety management function is responsible for identifying safety information and reporting/coordinating the information within the program office (systems engineering, quality, reliability, configuration management, procurement, etc.). The SSM also coordinates with the Staff System Safety Organization (SMC/SES) and the contractor(s) safety organization(s). This function ensures planning and implementation efforts satisfy program requirements. The Program Manager is responsible for ensuring that the System Safety function within his organization is properly staffed and resourced; should events warrant; failure to do so may be reported as a Program risk to the Program Executive Officer.

4.1.1 The System Safety Manager Roles and Responsibilities

The System Safety Manager is responsible for day-to-day management of the System Safety Program on behalf of the System Program Director/Manager. The SSM shall report high, serious, medium, urgent or improperly managed safety risks DIRECTLY to the System Program Director/Manager, and the SPO organizational chart shall clearly delineate this authority of the SSM. The scope of this responsibility includes coordination of government (SPO, Staff, and Range) activities, and oversight of contractor, sub-contractor, and vendor system safety efforts, to include flow down of safety requirements from the government to the contractor, sub-contractor, and vendor safety organizations and individuals throughout the lifetime of the system.

The SSM is also responsible for providing inputs for the staffing and financial budgets required to implement the system safety program. Examples of budgetary sub elements are:

- Necessary system safety manpower support (Government / Aerospace / SETA contractor)
- Any required system safety training;
- TDY attendance (SPO and invited guests) at any reviews, and meetings requiring system safety participation;
- Planning estimates of the Prime Contractor's system safety costs.

In addition, the SSM interfaces with other SPO organizations other aspects of system engineering, including configuration management , quality assurance, and reliability and maintainability to ensure that system safety engineering and policy requirements are included in all applicable SPO activities. The SSM interfaces with other SMC organizations including SMC/SE, and other SPO SSMs to identify common SMC system safety issues and to formulate system safety policy to resolve these issues. Also, the SSM interfaces with organizations outside of SMC to make system safety engineering policy facilitates tailoring of Range requirements, and to help ensure the contractor meets these requirements.

Typical roles of prime contractors include performance of technical analyses, and day-to-day participation in design and development efforts. Typical roles of government, SETA

and FFRDC personnel include requirements development and review and verification of a contractor's plans technical analyses and reports. Contractor and government personnel shall all typically participate in a single team effort for systems engineering, systems safety engineering and mishap risk control and acceptance. SMC/SE is available to assist system safety personnel in obtaining appropriate training.

Individuals assigned system safety responsibilities (e.g. both government and contractor) shall have the appropriate qualifications (See Table 1) to properly perform their system safety functions. SPO personnel shall also be properly trained on the SPO unique processes and tools. The SPD is responsible for properly equipping his personnel with the processes and tools (e.g. Hazard Log Database) needed to perform the work.

Qualifications for key system safety personnel shall include adequate education and training, experience and proven ability (through means such as certification) in order for each key person to fulfill his or her role.

TABLE 1 Minimum Qualifications

Government and Contractor Key System Safety Personnel*

Program Complexity and hazard potential	Education	Experience	Certification
High	BS in Engineering, Physical Science, plus training in System Safety++	Four years in system safety	Desired: CSP# or Professional Engineer Required: APDP Level 1 or equivalent
Moderate	Bachelor's Degree plus training in System Safety	Two years in system safety or related discipline	Enhancement: CSP or Professional Engineer. Required: APDP Level 1 or equivalent
Low	High School Diploma plus training in system safety	Four years in system safety	Required: APDP Level 1 or equivalent

* NOTE: Waivers shall be approved by the SMC Chief of System Safety at SMC/SE.

@ Most SMC programs are of high complexity and hazard potential. All programs shall be classified "High" unless justification is approved by the SMC Chief of System Safety at SMC/SE

CSP – Certified Safety Professional in System Safety Aspects

++ System Safety Training for government key system safety personnel (including at least one responsible full time System Safety Manager or System Safety Engineer per Systems Program Office, Joint Program Office or System Wing) shall include the USAF System Safety Analysis Course and System Safety Management course or NASA equivalents, relevant Space Safety and Explosives/Weapons Safety courses, plus other initial and update training provided through SMC/SE.

Acquisition Professional Development Program (APDP) Level Certification required for Government Personnel; equivalent required for FFRDC, SETA Contractors, etc.

4.1.2 MIL-STD-882C Tailoring and Associated CDRLs and DIDs

MIL-STD-882C, "System Safety Program Requirements", is the standard established by SMC for use in all Programs managed by SMC. MIL-STD-882C describes the management of all contractor system safety programs for the Department of Defense. The main portions of MIL-STD-882C are the Tasks and Data Item Descriptions (DIDs). As MIL-STD-882C discusses all system safety tasks, the entire document is not used for every system safety program. Therefore, the authors of the document made it mandatory to tailor for specific programs.

Each task within MIL-STD-882C can be tailored. Tasks are tailored (i.e., deleted, altered, or added) in order to better accommodate the program being supported. Tailoring allows for a system safety process that is customized to the specific Program, by which cost savings can be realized. It is the responsibility of the System Wing to ensure that funding is made available in order to perform those tasks listed in the Program's tailored MIL-STD-882C task list. The sections of tasks described by MIL-STD-882C include program management and control, design and integration, design evaluation, and compliance verification. . If a Government Statement of Work is included as of a Request for Proposal, then the tailored MIL-STD-882C task list is located as part of the section on System Safety.

The Contractor shall develop and implement a System Safety program, per the MIL-STD-882C (Tailored), that clearly states how their System Safety Program will be conducted, to include hazard analysis for the system throughout its lifetime, and will include software system safety.

The program shall include the necessary planning, coordinating, and engineering analysis to:

- Identify the safety-critical functions of the system and establish a protocol of analysis, design, test, and verification & validation for those functions.
- Tailor and communicate generic or initial safety-related requirements or constraints to the system and software designers as early in the life cycle phase as possible.
- Identify, document and track system and subsystem-level hazards.

- Identify the system-level effects of each identified hazard.
- Categorize each identified hazard in terms of severity and probability of occurrence (specify qualification or quantification of likelihood)
- Conduct in-depth analysis to identify each failure pathway and associated causal factors. This analysis will be to the functional depth necessary to identify logical, practical and cost-effective mitigation techniques and requirements for each failure pathway initiator (causal factor). This analysis shall consider all hardware, software, and human factor interfaces as potential contributors.
- Derive safety-specific hazard mitigation requirements to eliminate or reduce the likelihood of each causal factor.
- Provide engineering evidence (through appropriate inspection, analysis, and test) that each mitigation safety requirement is implemented within the design and the system functions as required, in order to meet safety goals and objectives.
- Conduct a safety assessment of all residual safety risk after all design, implementation, and test activities are complete.
- Conduct a safety impact analysis on all Software Change Notices (SCN) or ECP for engineering baselines under configuration management.
- Submit for approval to the certifying authority, all waivers and/or deviations where the system does not meet the safety requirements or the certification criteria.
- Submit for approval to the acquiring authority an integrated system safety schedule that supports the programs' engineering and programmatic milestones.

Execution of system safety tasks by the Contractor is typically demonstrated by the generation of contract deliverables. The Contract Data Requirements List (CDRL) is a list of authorized data requirements for a specific procurement that forms a part of the contract. It is comprised of either a single DD Form 1423, or a series of DD Forms 1423 (individual CDRL forms) containing data requirements and delivery information. The CDRL is the standard format for identifying potential data requirements in a solicitation, and deliverable data requirements in a contract. System safety CDRLs should be linked directly to MIL-STD-882C tasks.

Data Item Descriptions (or DIDs) describe the data content and format. The most common Data Item Descriptions are described below:

DI-SAFT-80100A System Safety Program Plan (SSPP). This plan details the tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate or control hazards throughout the system lifecycle. The purpose of this plan is to provide a basis of understanding between the contractor and the managing activity to ensure that adequate consideration is given to safety during all life cycle phases of the program and to establish a formal, disciplined program to achieve the system safety objectives.

DI-SAFT-81300 Mishap Risk Assessment Report (MRAR). This Data Item report describes format and content preparation instructions for data resulting from the work tasks described in MIL-STD-882C Tasks 201- Preliminary Hazard List; 202 –

Preliminary Hazard Analysis; 203 - Safety Requirements/ Criteria Analysis; 204 – Subsystem Hazard Analysis; 205 - System Hazard Analysis; 206 - Operating and Support Hazard Analysis; 207 – Health Hazard Analysis; 301 - Safety Assessment; 302 – Test and Evaluation Safety; 303 – Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Request for Waiver/ Deviation; 401 – Safety Verification; 402 – Safety Compliance Assessment; 403 – Explosive Hazard Classification and Characteristics Data. The data resulting from these tasks and compiled into the MRAR are applicable to the system design, test, processing and operations within a contract.

DI-SAFT-80102A Safety Assessment Report (SAR). This Data Item report is a comprehensive evaluation of the safety risks being assume prior to test or operation of the system or at contract completion. It identifies all safety features of the system, design, and procedural hazards that may be present in the system being acquired, and specific procedural controls and precautions that should be followed.

DI-SAFT-80101A System Safety Hazard Analysis Report (SSHAR). This Data Item report documents hazard analyses that are used to systematically identify and evaluate hazards both real and potential, for their elimination or control.

DI-SAFT-80103A Engineering Change Proposal System Safety Report. This Data Item report is used to summarize results of analyses, tests and tradeoff studies conducted on proposed engineering design changes throughout the system life cycle.

DI-SAFT-80104A Waiver or deviation System Safety Report. This Data Item report summarizes the results of analysis, test, and tradeoff studies as they relate to a request for waiver/ deviation. It will identify the risk assessment, mishap potential, and justification associated with results of each waiver or deviation request received throughout the system life cycle.

DI-SAFT-80105A System Safety Program Progress Report. This SSPPR Data Item can be used to cover periodic reviews of safety activities and to monitor progress of contractor system safety efforts.

DI-SAFT-80106A Health Hazard Assessment Report. These HHAR Data Items are used to systematically identify and evaluate health hazards, evaluate proposed hazardous materials, and propose measures to eliminate or control these hazards through engineering design changes or protective measures to reduce the risk to an acceptable level.

DI-SAFT-80931 Explosive Ordnance Disposal Data. This Data Item data is used by the Naval Explosive Ordnance Disposal Technology Center (NAVEODTECHCEN) to develop, test, validate and publish joint service non-nuclear explosive ordnance disposal (EOD) 60 series technical orders. EOD technicians will use this data in support of testing, development and operational evaluation of new or modified weapon systems, ordnance items and aerospace systems.

DI-SAFT-81299 Explosive Hazard Classification Data. The purpose of this Data Item data is to obtain the necessary information for assigning hazard classification, such as hazard class/ division, storage compatibility group, and Department of Transportation (DOT) marking. These classifications establish the procedures for the storage and transportation of the item for all user elements.

At SMC two types of system safety programs are defined, based on the level of system safety to be performed. These are the large program (which is applicable to satellites and launch vehicles), and the small program (which is applicable to user segment items and some ground segments). For each type, a template tailoring for both tasks and DIDs have been constructed by SMC/SE and can be found in the appendix.

The relationship between MIL-STD-882C Tasks and the DIDs that support them can be summarized below:

MIL-STD-882C Tasks and DIDs Matrix		
<i>Task Description</i>	<i>DID No.</i>	<i>DID Description</i>
101 - System Safety Program	DI-SAFT-80100A	System Safety Program Plan
102 - System Safety Program Plan	DI-SAFT-80100A	System Safety Program Plan
103 - Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms	Not Applicable	Not Applicable
104 - System Safety Program Reviews/ Audits	Not Applicable	Not Applicable
105 -System Safety Group/System Safety Working Group Support	Not Applicable	Not Applicable
106 - Hazard Tracking and Risk Resolution	DI-SAFT-80105A	System Safety Program Progress Report
107 - System Safety Progress Summary	DI-SAFT-80105A	System Safety Program Progress Report
201 - Preliminary Hazard List	DI-SAFT-80101A	System Safety Hazard Analysis Report
202 - Preliminary Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
203 - Safety Requirements/Criteria Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
204 - Subsystem Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
205 - System Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
206 - Operating and Support Hazard Analysis	DI-SAFT-80101A	System Safety Hazard Analysis Report
207 - Health Hazard Assessment	DI-SAFT-80106A	Health Hazard Assessment Report
301 - Safety Assessment	DI-SAFT-80102A	Safety Assessment Report
302 - Test and Evaluation Safety		
303 - Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/Waiver	DI-SAFT-80103A	Engineering Change Proposal System Safety Report
	DI-SAFT-80104A	Waiver of Deviation System Safety Report
401 - Safety Verification	DI-SAFT-80102A	Safety Assessment Report
402 - Safety Compliance Assessment	DI-SAFT-80102A	Safety Assessment Report
403 - Explosive Hazard Classification and Characteristics Data	DI-SAFT-81299	Explosive Hazard Classification Data
404 - Explosive Ordnance Disposal Data	DI-SAFT-80931	Explosive Ordnance Disposal Data
Multiple Tasks	DI-SAFT-81300	Mishap Risk Assessment Report

Conversely, a matrix showing how each of the DIDs supports the various MIL-STD-882C tasks is located in the Appendix.

4.1.2.1 Compliance and Reference Documents

The following compliance and reference documents shall be included as part of the Request for Proposal:

Compliance:

- MIL-STD-882C “System Safety Program Requirements”, (Tailored).
- AFSPCMAN 91-710, “Range Safety User Requirements” (Tailored).

Reference:

- AFI 91-202 (AFSPC Sup June 2005) Chapter 9, System Safety and 11, Space Safety
- AFI 91-204 (AFSPC Sup January 2007) Chapter 8, Missile Mishaps; Chapter 9, Space (and Orbital) Mishaps
- AFI 91-217 Space Safety and Mishap Prevention Program
- AFMAN 91-222, Space Safety
- SMC/CV Policy Letter, Mishaps at Contractor Facilities

Note that while the pertinent AFI are used as references for the purposes of the RFP, they are still considered compliance documents to the Program Office. It is the responsibility of the Program Office to ensure that requirements imposed on the Program offices by Air Force Instructions be implemented by the contractors through proper flow down of requirements and contractual language.

4.1.2.2 Other RFP/Contractual Items

Other contractual items for the RFP that require system safety involvement include:

- Statement of Objectives (SOO)
- Government or Contractor Statement of Work
- Award Fee
- Federal Acquisition Regulations (FARs)
- DOD Contractor’s Safety Manual for Ammunition and Explosives
- Technical Requirements Document (TRD), System and Subsystem Specs, Interface Control Documents
- Sample or Reference Mission(s)
- Tasks
- Task Tailoring
- Indemnification Strategy
- Acquisition Strategy and Template
- Line items

4.1.3 Request for Proposal Instructions to Bidders (RFP Section L)

SMC/SES provides a list of safety items that apply to Section L of the RFP, and can assist in the drafting of particular bidder instructions by providing recommended input. The following list of safety items shall be tailored to meet RFP requirements:

- Have the Contractor describe the proposed system safety program strategy, methodology, process, major tasks, resources, techniques, tools and criteria to be used to assure the end product meets all of the program safety and mishap risk management requirements of MIL-STD-882C;
- Have the Contractor describe his relevant lessons learned;
- For Launch Vehicle programs, have the Contractor describe how he plans to support the SPO efforts to satisfy range safety requirements;
- For payload programs, have the Contractor describe how he plans to support the SPO efforts to satisfy payload range requirements;
- For ground control, network and facility systems, have the contractor describe his plan to support the SPO efforts to satisfy system safety requirements and obtain approval/certification;
- For all programs, have the contractor describe his plan to facilitate government system safety insight of all relevant contractor system safety activities. Include verbiage on qualified personnel Qualified personnel shall meet the requirements of Table 1 of this regulation.
- For all programs, have the contractor discuss the proposed approach to developing an Integration, Test and Evaluation (IT&E) strategy will be evaluated. It must include system safety in a comprehensive, thorough, integrated, and documented program T&E plan;
- For all programs, have the contractor discuss the proposed approach to develop an integrated training program, which includes system safety, will be evaluated.

4.1.4 Request for Proposal Evaluation Criteria and Standards (RFP Section M)

Typically, evaluation criteria and standards for system safety are included under the program management and system engineering sections. The following list should be included in Section M for system safety:

- Contractor's detailed description of his System Safety Program. Define the approach and the specific processes, methodologies, major tasks, resources, techniques, tools, and criteria used to develop and implement his system safety program will be evaluated against criteria within MIL-STD 882C;
- Contractor's description of the process by which the system safety program will be integrated with the requirements development, system definition, system design, operational design, and hazard/risk management processes will be evaluated;
- Contractor's proposed systems engineering process will be evaluated on how it integrates the system safety requirements;

- Contactor's proposed approach to developing an Integration, Test and Evaluation (IT&E) strategy will be evaluated. It must include system safety in a comprehensive, thorough, integrated, and documented program T&E plan;
- Contactor's proposed approach to develop an integrated training program, which includes system safety, will be evaluated;
- Contractor's description of how he plans to support the SPO efforts to satisfy range safety requirements for payload or launch vehicles depending on the SPO mission will be evaluated;
- For ground control, network, and facility systems, contractor's detailed planning to support the SPO's efforts to satisfy system safety requirements and obtain approval/certification will be evaluated;
- Contractor's description of lessons learned will be evaluated;
- For all programs, the contractor's description of his plan to facilitate government system safety insight of all relevant contractor system safety activities will be evaluated.

4.1.5 Work Breakdown Structure (WBS)

The Government SSM/SSE must ensure in the RFP's bidder's instructions that the contractor provides for a specific system safety WBS element. The contractor's work breakdown structure (CWBS) shall identify safety elements (tasking and level of effort) and shall be consistent with system engineering requirements and schedules. The Government SSM shall be familiar with the detailed descriptions of both the Government's and contractor's WBS, and shall ensure that system safety is included in the WBS and that adequate resources are allocated in order to support system safety activities throughout the Program.

4.1.6 The System Safety Management Plan and Task Planning

System safety management requirements and tasks will be placed into the SPO System Safety Management Plan. Each Government system safety management plan (SSMP) shall, as a minimum, include:

- Organizational responsibilities;
- Personnel qualifications (see Table 1 of this SMC Instruction);
- Manpower authorizations by skill types need dates and required training;
- Resource loading including manning and funding for the life cycle;
- Authority and Accountability for implementing tasks and risk decisions;
- Status assessment of controls/mitigation;
- Schedule control and reporting;
- Beginning and ending milestones for the task;
- Required management and technical reviews;
- Planned approach and methods of task accomplishment;
- Interfaces with related efforts such as contractor system safety programs and plans.

Both Government and Contractor System Safety tasks shall be integrated into the program Integrated Master Plan and into the Integrated Master Schedule (IMP and IMS). Contractor's work packages shall be consistent with the Government's system safety tasks. The System Safety task scheduling shall guarantee timely safety risk identification and control information to support valid management decision making. The task schedule shall include: task title, phase (such as Pre-A, A, B, C, or D), milestone definitions, and inter task dependencies.

The SSMP shall be prepared by the System Wing SSM and approved by both the SPD and SMC/SE.

Each contractor system safety task is authorized by inclusion in the government approved, contractor created SSPP. Contractor plans and Contract Data Requirements Lists (CDRLs) are also approved and signed by the contractor's management, empowering the contractor SSM. Follow-on contractor tasks are authorized by contract change(s) and documented by changes to the approved SSPP. The initial release of the government SSMP authorizes the initial set of government system safety tasks. The government SSM shall be given the appropriate authority, resources and responsibility to implement the SSMP.

The status of each system safety task will be reflected in the SSPP updates, CDRL items submittals, IMP and IMS in accordance with the contract.

4.1.7 Risk Ranking, Tracking, and Residual Risk Acceptance

The SPO shall develop and implement an integrated hazard/risk tracking process. The government shall play an active role to protect the integrity of this process. The results of this process shall include the hazardous conditions/actions, hazard causes, hazard effects, hazard controls, risk ratings before and after the proposed control(s), risk and cost effectiveness ranking, hazard control verifications and documentation. The identified hazards and mitigations shall be tracked and managed throughout the entire program life.

The SPO manages the system safety hazard/risk identification and mitigation. Risk handling, abatement, control, and/or resolutions strategies shall be implemented to identify, evaluate, manage and/or resolve each risk, consistent with performance, cost and schedule.

Acceptance of residual risk shall be accomplished by signature of the appropriate managerial authority on a hazard report, as shown in Appendix A.

Acceptance of residual risk shall be accomplished by signature at the appropriate managerial authority on a hazard report, as illustrated in Appendix A.

4.1.8 Meetings

The Government SSM and staff from SMC/SE shall be allowed access to, and shall participate in government / contractor design reviews, technical interchange meetings, management status reviews, source selection boards, system safety group meetings and system safety working group meetings, and any other meetings held by the SPO that may be germane to system safety, as determined by SMC/SE. A system safety manager representative shall be included as a member of Program Engineering Change Proposal review and Configuration Control Boards.

4.1.8.1 The System Safety Group

A System Safety Group (SSG) will be established (IAW AFI 91-202 AFSPC Sup, Chapter 9) for each SMC Acquisition Category I (ACAT 1) or equivalent programs and for all SMC missile, launch vehicle, satellites and ground facilities (at the SPO level if programs are smaller) unless waived by the AFSPC/SES through SMC/SE. The SSG is the method used by senior leadership to provide guidance and oversight to the SPO's system safety program. The SSG will consist of the SPD/Program Manager, the SMC Chief of System Safety, the Program System Safety Manager, and representatives from the using organization (i.e., HQ AFSPC, Numbered Air Force (NAFs), Centers, Space Wings), Air Force Operational Test and Evaluation Center (AFOTEC), HQ AFSC and other DoD operators, users, and industry organizations.

The SSG activities shall be embedded in the Program Office System Safety Management Plan and explicitly supported by line items in the Contract Data Requirements List and tasks in the Request for Proposal and contract Statement of Work. In turn, the contractor should include SSG support activities in the IMP and IMS. The SSG/SSWG shall include participation from all SPO stakeholders' organizations. Attendance at any SSG by SMC/SE personnel shall be funded by the SPO.

The Program Manager or the Deputy Program Manager chairs the SSG. The SSG meets as required (at least annually) at the request of the government program manager. Any member of the SSG may request that the program manager call a meeting.

The SSG develops and coordinates the SSG Charter. The SSG Charter will address the purpose and scope, operating procedures, administration of the SSG and SSG membership. The SSG membership includes program, center, HQ AFSPC, and HQ AFSC.

The SSG is responsible for the following:

- Evaluating the program System Safety status including funding;
- Ensuring all appropriate managers consider and document the residual risks of hazards;

- Reviewing the analyses of major safety design trade-offs and modifications. These analyses will include hazard risk descriptions, proposed corrective actions and their effect and current status;
- Reviewing the status of planned, pending, active, and disapproved safety modifications;
- Reviewing and possibly approving selected hazard analysis and their recommended controls and verification;
- Reviewing high accident potential reports that have occurred since the last meeting;
- Reviewing User/operator issues;
- Reviewing the action item summary including action agencies and suspense dates. Include old and new action items;
- Developing and maintaining the SSG charter. The SSG charter will address the purpose and scope of the SSG, SSG membership, operating procedures, and administration of the group;
- Identifying and establishing System Safety Working Groups as necessary, to work detailed safety risks.

The SPO program manager will be responsible for preparing minutes of SSG meetings and distributing them to SSG members and attendees within 30 days of the meeting. SSG minutes shall be sent to SMC Safety Office (SMC/SES). If a SSG is not held on a major program within a year of the previous meeting from the last one an explanatory letter shall be sent to HQ AF Safety Center and a copy to AFSPC/SES).

4.1.8.2 The System Safety Working Group

IAW AFI 91-202, the government SSWG is established by the SSG to work detailed safety issues. It is chaired by the government SSM and does not generally require the attendance of the SPD or Program Manager. Typical SSWG activities include: assessing the status of safety activities in the total system, various system segments, elements, subsystems and components. Hazards and their mitigations are reviewed and disposed as follows:

- Ill-defined hazards are returned to the originator for clarification;
- Valid hazards for which mitigation proposals have not been made shall be assigned to an action officer, for mitigation;
- Valid hazards that have been completely mitigated are recorded; a residual risk acceptance form is generated and presented to the appropriate risk acceptance authority for signature, and monitored;
- Valid hazards that have been partially mitigated are documented, assigned to an action officer and monitored;
- Non-valid hazards are documented and archived.

Typical SSWG members are government and contractor SSM, contractor specialists, SMC staff system safety engineers (SMC/SES), program office engineers, and range

safety personnel. Specific attendance at an SSWG meeting will depend on the nature of the issues and support required by the SSWG.

The SSM shall ensure that minutes of meetings shall be prepared and distributed to members and attendees within 30 days after the date of the meeting

System safety reviews, SSG/SSWG meeting minutes, and audit/inspection results will be written, distributed and stored in the system safety library.

4.1.9 System Safety Information Architecture and Maintenance

The SPO activities shall include a process for collecting, reviewing, auditing, analyzing, and sharing of system safety information and lessons learned. Required components can include, but are not limited, to:

- System Safety Management Plan (SSMP) / System Safety Program Plan SSPP;
- Preliminary Hazard List;
- Preliminary Hazard Analyses (system safety, explosive safety and bioenvironmental);
- Hazard Analysis;
- Hazard Reports;
- Hazardous Material Management Program Report (HMMPR);
- Hazard Risk Assessment Matrix (HRAM);
- System Safety Status Report;
- Mishap Risk Assessment Reports (MRARs);
- Missile System Pre-launch Safety Packages (MSPSPs).

4.1.9.1 Hazard Tracking Log

A hazard and mitigation tracking system shall be implemented as part of the system safety process. The SSM is responsible for developing (when necessary) and implementing tracking procedures for all identified hazards and their solutions, when feasible or applicable. The SPD, PM and SSM shall ensure that follow-up/close-out actions are appropriately tracked and documented. The SPD, PM and SSM shall ensure that management decisions for acceptance of residual risks are documented. The hazard tracking system must provide “closed-loop” feed-forward/feedback control of hazards to assure that, for example:

- Safety recommendations are actually implemented as hazard controls,
- Test information is used to confirm or update system safety analysis,
- Safety risks and safety control system performance levels, as determined by system safety analyses, are validated or upgraded with ongoing mishap and system performance information.

Part of this tracking should occur through the generation, use and approval of analysis documents such as signed hazard reports (see example in Appendix A). However a

Hazard Tracking Log (or Hazard Control Verification Log) is used later in the tracking process to assure that controls identified for each hazard are actually implemented.

The Hazard Tracking Log summarizes each hazard and highlights those that are not formally closed. Hazards noted in the Hazard Tracking Log are annotated with Hazard Risk Indices (also known as Hazard Risk Assessment Values or Risk Assessment Codes). The Hazard Tracking Log is used to track both design related and operationally related hazards. All hazards which have not been closed at the time of issue of the most current system safety analysis document (such as MRAR or MSPSP) shall be summarized in the hazard log. Hazards will be tracked from their identification (in the various hazards analyses, tests or operational experiences) throughout the system life cycle. Hazard log entries shall be continuously available for reference, and open entries shall be presented at key milestones including program reviews. All identified hazards will be verified closed prior to the mission. Closure of each hazard will be denoted by the signature of appropriate contractor and government management on the associated hazard report. A hazard will be considered closed only when the cognizant safety organizations and program management have determined that one or more of the following requirements are met:

- The hazard has been eliminated through design, and the design action is
- verified, or,
- The hazard has been reduced to an acceptable level in accordance with the system safety order of precedence and the level of reduction has been suitably verified, or,
- The hazard has been assessed and noted. The risk has been accepted by contractor and government program offices and other stakeholders through the safety review process.
- Safety concerns affecting schedule, cost, system safety precedence, or requiring deviation or waiver to safety requirements are appropriately resolved.

While historically paper forms have been used to track hazards, SPOs and other organizations conducting acquisition functions are authorized and encouraged to operate and maintain hazard risk tracking database software. Hazard log contents may include the following:

- System/Subsystem Name:
- Hazard Report Number:
- Hazard Report Title/Description:
- Current Status:
- Date Opened:
- Date Closed:
- Responsible Party:
- Description of Recommended Controls:
- Identification and Description of Residual Risk:
- Closure Approval (Contractor / Range / Operational Safety / Government Program Office)

It is the responsibility of Program Office to maintain and use a log of all identified hazards and residual mishap risk, as part of their overall System Safety management plan. This function shall not be delegated to contactors, and shall be under the direct cognizance of the Program Office.

4.2 System Safety Engineering

The system safety engineering function requires specialized knowledge and skills in applying engineering principles and techniques to identify, and eliminate or control system hazards and hazardous conditions, and verify the hazard mitigation.

4.2.1 System Safety Engineering's Role in Systems Engineering

System safety is involved in systems engineering throughout the lifecycle, and system safety should be embedded as early as possible in the design. The System Safety Engineer (SSE) performs analyses and makes technical recommendations throughout the life cycle, i.e., from concept design, development, build, operations, sustainment, and disposal. Technical documents shall be reviewed, evaluated, and corrected by the SSE to ensure design safety has been implemented. System safety approval shall be required for release of drawings, specifications, computer source code, procedures, and other program documentation that the SSE decides has potential system safety impact or designates as safety-critical.

The SSE interfaces with personnel from other specialties and will participate in milestone reviews. The SSE should also work with operational safety organizations and gather lessons learned throughout operations and disposal. Safety engineering data should be obtained from:

- Existing analyses from other fields (such as FMECA from reliability);
- Requirements (Air Force Instructions, MIL-STD's, etc.);
- Mishap, HAP and incident/anomaly data;
- Lessons learned from similar or previous programs.

The SSE shall establish system safety design criteria. Recommendations for new system safety design criteria will be made using studies, analyses and test data. System Safety shall use these criteria to further evaluate requirements to see if they are adequate, inadequate, or overly restrictive. System Safety shall use the Engineering Change Process to incorporate appropriate system safety related changes.

System Safety engineering tasks shall provide controls and verifications for hazards identified by hazard analyses and/or failure analyses. The results of the system safety process shall be documented.

Non-Developmental Items (such as Commercial Off-the-Shelf or COTS, and Government Furnished Equipment or GFE), systems, components, equipment shall be analyzed for the intended use to identify and resolve hazards.

A software safety engineering program shall fully support the existing system safety engineering program and functionally link software architecture to hazards and their failure pathways. All computer software elements must be identified and must be placed under software configuration control. System safety design requirements must be properly incorporated into the software and supporting documentation.

System safety deficiency reports submitted by operations and support personnel shall be analyzed for possible design or equipment changes.

Procedures and results of contractor inspections and tests must be reviewed in order to ensure that acceptable levels of safety are maintained. This includes major or critical characteristics of system safety significant items that deteriorate with age, environmental conditions, or other factors.

4.2.1.1 Requirements Review, Allocation, and Traceability

Upon request, SMC/SES will provide a list of safety requirements documents for use by the SMC program office. The Program's uniquely tailored documents shall be periodically updated as baselines, configurations, performance, and processes change. The following list identifies some of the Contractor-generated safety requirements documents:

- The System Safety Program Plan, which demonstrates how the Contractor supports the Government system safety program;
- The Hazardous Material Management Plan, which demonstrates how the Contractor supports the government hazardous material management program portion of the Government SSMP;
- Hazard Reports and Hazard Analysis Reports, which define the safety risks found in the Program, and their associated controls.

Safety-related requirements can also be found in the Technical Requirements Document, and system and sub-system specifications.

There are also requirements that can be traceable to external documentation, such as:

- AFI 91-202 AFSPC Sup 1: "USAF Mishap Prevention Program"
- AFI 91-204: "Safety Investigations and Reports"
- MIL-STD-882C: "System Safety Program Requirements"
- MIL-STD-1522B: "Design and Operations of Pressurized Missile and Space Systems"
- MIL-STD-1540: "Test Requirements for Launch & Space Vehicles"
- MIL-STD-1576: "Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems"

System safety is heavily involved in the requirements process. Activities include:

Review - The SSE shall review appropriate Program documentation to ensure system safety requirements have been properly incorporated.

Allocation - The SSM/SSE ensures that tasks are allocated from safety requirements to the system specifications, the Contractor Statement of Work (CSOW) and other documents. The system safety engineer will also ensure that system safety tasks are allocated to other disciplines, facilities and organizations. – This includes requirement allocation, hazard analyses, data, test, configuration control, and facilities.

Traceability - The system safety engineer will ensure that the system safety requirements are traced to the appropriate specification. This system safety manager will also ensure that the responsibility for safety concerns is assigned to the appropriate organization (vendor, contractor or government).

4.2.1.2 Change Control

The system safety engineer is responsible for the review of design changes for system safety impacts, which includes system safety inputs for recommended changes and/or corrective actions associated with change activities. System safety impacts of proposed design changes shall be considered in all government/contractor configuration control board actions. A system safety assessment of design changes with recommended mitigations should be provided to the program manager and the systems engineer. Government system safety engineer shall be authorized to participate in both government and contractor configuration control board meetings.

4.2.2 Hazard Analysis and its Techniques

Hazard analysis techniques are used to identify hazards and in some cases determine the mishap risk. These techniques include historical record review, what-if analysis, fault tree analysis, failure modes and effects criticality analysis, event tree analysis, energy flow/barrier analysis, cause consequence analysis, and sneak circuit analysis.

Mishap risk processes and criteria/thresholds should be defined before or during most of these analyses.

4.2.2.1 Historical Record Review

In this technique, the analyst reviews hazards, hazard controls, verifications, and mishaps of systems which are similar to the one to be designed and built. The analyst then uses analyses which are applicable to his system. The advantage of using this technique is that

if there is enough similarity between the new and old systems, the analyst has a good start at identifying and controlling the hazards of the new system.

A disadvantage of using this technique is that although the systems being reviewed may seem similar to the system to be designed, the analyst shall also ensure that hazards from the old systems are not being designed into the new system and also that hazards in the new system not present in the old system are identified and controlled.

4.2.2.2 Safety Requirements Analysis

Safety Requirements Analysis is performed in order to identify, document and ensure satisfaction of safety requirements and criteria necessary for control of hazards to an acceptable level. The requirements and criteria may relate to specific hazards that have been identified, or may be safety related but not necessarily tied to a specific hazard. The analysis includes the following activities:

- Determination of applicable generic system safety design requirements and guidelines from sources such as federal, military, national and industry regulations, instructions, codes, standards and specifications; incorporation of these requirements and guidelines into the high level system specifications and design documents as appropriate.
- Deriving additional requirements and specifications, using available hazard analyses and the system segments, subsystems, hardware, software, interfaces, etc.

Typical results of the Safety Requirements Analysis include a summary or a total listing of generic requirements sources used, and of specific applicable requirements and criteria identified during the analysis. In addition to analyzing the requirements, the SSE shall ensure that these safety requirements are properly translated into system hardware and software requirements and guidelines, where appropriate, and placed under configuration control. The SSE shall also ensure that these safety requirements are implemented in the system's design, development, test, operating instructions and training.

The technique is typically not used as a stand-alone task on space systems. Examples of this technique found in are tailoring of AFSPCMAN 91-710 requirements and of MIL-STD-882C tasks. Safety Requirements Analysis is one of the techniques typically employed in generating a PHL/PHA. Details for successful employment of RA as part of a separate task can be found in MIL-STD-882C as Safety Requirements and Criteria Analysis (SRCA, Task 203). As a separate task SCRA is particularly useful for systems such as facilities whose safety features can be largely determined using regulatory or code requirements. For unique and complex space and weapon systems the RA technique shall typically be supplemented by other techniques. Using techniques such as a "What-If" analysis or Energy Flow/Barrier Analysis in conjunction with Requirements Analysis helps ensure that hazard risks that regulators could not have foreseen are mitigated.

4.2.2.3 What-If Analysis

What-If Analysis can be used to identify situations or events that could produce undesired consequences. In this analysis, the input of the analysis team member(s) is captured in a brainstorming environment. First the boundaries and ground rules for the analysis are established. Then what-if questions are asked by group members concerning system or subsystem failures. Some what-if analyses are documented in a narrative format, many people find a matrix table easier to use.

The what-if process can be used during any stage of the design and applied to almost any system level, system process, or operation. The technique is not difficult to use. The technique helps the analyst focus on details of the system and operation, and allows team experience to be used creatively to find hazards and potential controls. The experience and diverseness of the team are critical to ensure the effectiveness of the analysis. All appropriate backgrounds (technical, operational ...) should be included.

Limitations of the What-If technique are that it is a qualitative process which leads to qualitative answers, that it is unstructured compared to some similar techniques, and that comprehensiveness is not assured. Generally What-If Analysis is only the start of a hazard analysis process. Also, if combined failures are to be considered, then a different or supplemental analytical technique is advisable. What-If Analysis is often combined with a checklist, such as may be obtained using requirements analysis, to help ensure comprehensiveness.

4.2.2.4 Energy Flow/Barrier Analysis (EF/BA)

During Energy Flow/Barrier Analysis, the SSE identifies as many potential sources of unwanted energy flow as possible, and ensures that the “barriers” are adequate. The steps are:

- Identify as many energy sources in the system as possible. Energy sources may be of many types including electrical, mechanical, chemical, and others.
- Examine the potential for unwanted energy flow from each source to any personnel or hardware that could be lost or damaged due to a mishap.
- Identify existing controls (“barriers”) to each potential unwanted transfer of energy. In this context the term “barrier” may include physical barriers such as walls, insulations, or shielding, that limit the transfer of energy. “Barrier” may also refer to analogous controls like limited source energy or exposure time, or increased distance.
- The SSE then establishes strategies for reducing the hazard risk from undesired energy flows to acceptable levels or better. These strategies typically involve the use of one or more “barriers” in addition to those already present. The SSE proposes strategies (or combinations of strategies) and management accepts the best one based on criteria such as mishap risk, cost effectiveness and feasibility (including schedule).

EF/BA is often used during performance of a Preliminary Hazards List or a Preliminary Hazards Analysis. Limitations of the method are that certain types of hazards, such as confined space asphyxia and operator fatigue, cannot be detected by this method. Also, barriers/controls such as smoke detectors and surge protectors defy easy classification. Results of the EF/BA are typically combined with those of other basic techniques and reported in the PHA.

4.2.1.5 Failure Modes, Effects and Criticality Analysis (FMECA)

The FMECA technique examines and documents the possible ways in which a system component, circuit, or piece-part may fail; and the effect of the failure on system operation. It is closely related to Failure Modes and Effects Analysis (FMEA), which is FMECA without a criticality analysis. Criticality analysis makes FMECA significantly more useful to System Safety Engineers than FMEA is. The FMECA is typically initiated and used by reliability personnel to provide reliability calculations using quantified data, to determine likely effects of failures on the system, and to document single-point failures. A failure is the inability of a system, subsystem, component or part to perform its required function on demand, within specified limits, under specified conditions and for a specified duration. The tasks involved in FMECA include

- Identifying the component;
- Identifying the failure mode (how the component could fail);
- Identifying the failure cause or mechanism (why the component could fail);
- Identifying failure effects (the results of a potential failure);
- Estimating criticality (how bad the failure would be perhaps in terms of a risk priority rating);
- Establish failure probability (qualitative or quantitative);
- Recommending corrective actions.

The results of the FMECA are typically recorded in a matrix that include columns for part names and numbers, potential failure modes, causes, effects, failure probability, risk priority ratings, recommended improvements, and risk priority rating after the improvement.

FMECA can be performed at almost any point in the program. The FMECA can be more detailed when performed late enough in the program that system components and parts are known. While the FMECA is typically not initiated by safety personnel, the FMECA results provide hazard information that can be used by system safety analysts. FMECA results can be particularly useful when performing Fault Tree Analysis and Fault Hazard Analysis. The benefits of the FMECA include:

- Discovery of potential single-point failures and assessment of the risks;
- Optimization of reliability;
- Design evaluation and improvement;
- High risk hazards found in a hazard analysis can be analyzed to the piece-part level.

Some of the limitations of the FMECA include:

- Inability to combine the effects of coexisting failures;
- Extraordinarily tedious and time consuming, for complex systems;
- Failure probabilities can be difficult to obtain.

4.2.2.6 Fault Hazard Analysis (FHA)

Fault Hazard Analysis is performed during design to identify, evaluate and control hazards resulting from piece-part or component faults. This technique was derived from FMECA in order to address categories of faults other than malfunctions. FHA emphasizes those results with safety impacts, and also addresses the effects of single faults.

A fault is a normal, abnormal or inadvertent activation of a component or human function that (singly or in combination with other failures/faults) may result in mishap loss. Fault is a more general term than failure.

The FHA builds on available data such as program specifications and requirements, design drawings, functional diagrams and descriptions, interface control drawings, failure reports, and results of the PHA and FMECA. The FHA process can be summarized as follows:

- Identifying the fault;
- Identifying the fault cause;
- Identifying the fault cause for safety critical component fault conditions and safety critical operations/functions;
- Identifying the fault cause for environmental effects (exposure of susceptible component to environment);
- Describing the hazardous condition created;
- Describing the potential undesired effects of the hazardous condition;
- Determination of the severity level or Hazard Risk Assessment Value (see Appendix A6);
- Specifying hazard elimination/control provisions;
- Verifying closeout status of the hazard.

The results of the FHA are often recorded in a matrix format that lists by system/subsystem the fault, fault cause, hazardous condition, undesired effect, Risk Assessment Code, controls, and verification. Other formats used for input to or output from an FHA include the Hazard Report and/or Hazard Analysis Report.

Fault Hazard Analysis is widely used for space and missile systems, due to the requirement for high mission success (FHA is typically used after a PHA has been performed in order to help complete a subsystem or system hazard analysis). FHA has advantages over FMECA for safety analysts because it looks for other faults (e.g., human error interface compatibility) in addition to component failures, and focuses on safety-

related events. The FHA can be used to look at faults that could occur in any phase of the system life cycle.

4.2.2.7 Fault Tree Analysis (FTA)

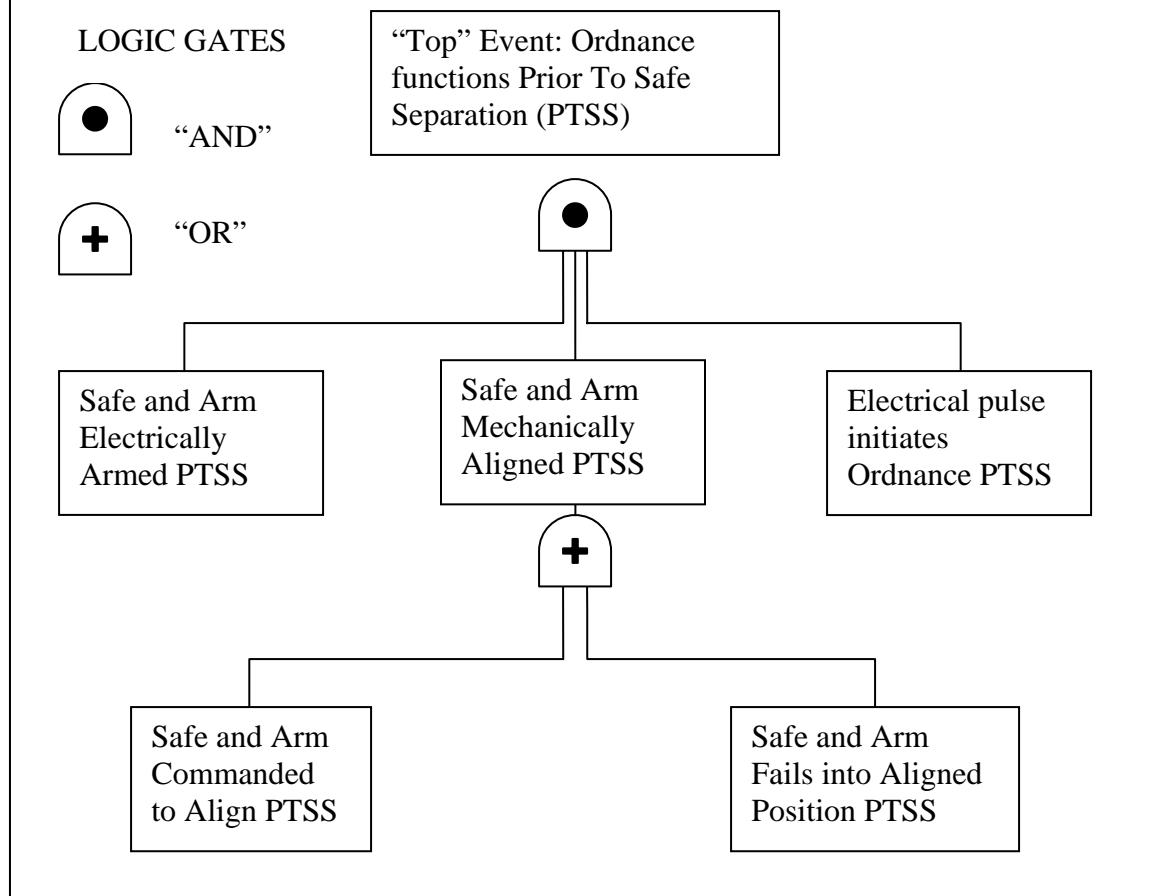
Fault Tree Analysis is performed to:

- Systematically deduce the necessary and sufficient faults that would result in a defined “top” undesired event;
- Document the results in a graphical Boolean logic tree and/or logical expression;
- Provide for potential quantitative probability determination;
- Enable efficient prevention or control of the probability of the “top” undesired event.

The Fault Tree Analysis process includes constructing and using a Fault Tree as follows:

- Identifying the “top” undesired event;
- Identifying the first-level contributing fault events or conditions (causes);
- Linking contributing faults (causes) to the top undesired event using a logic gate (e.g. “and” or “or” gate);
- Identifying second-level contributing fault events or conditions (causes);
- Linking second-level contributing faults (causes) to first level by logic gate;
- Decomposition at lower levels until satisfactory initiating fault events (root causes) are obtained, or a limit of scope of analysis is reached;
- Simplifying the resulting logic diagram and Boolean expression to obtain minimum “cut sets”, showing the minimum necessary and sufficient faults (causes) to cause the “top” undesired event to happen;
- Use the cut sets to determine the possible improvements from preventing contributing faults (causes), and/or continue to quantify the probability of a top event occurring.

An example Fault Tree Diagram of an ordnance function is given in Figure 4.

FIGURE 4: EXAMPLE FAULT TREE DIAGRAM

Results of an FTA include a logic diagram (“fault tree”) and a logical expression of the faults that would be necessary to cause the “top” undesired event. Results may also include a probability that the “top” undesired event will occur. The most important result is often an improved understanding of a complex system, obtained during the systematic detailed analysis of its fault events and conditions.

Fault Tree Analysis is used when the SSE desires to consider the effects of multiple faults occurring together, in addition to single faults. The FTA can be used at any point in the system design and analysis but is most often applied during subsystem and system hazard analysis at a time when a large number of design details are available to complete the tree. The FTA focuses on deductively finding events that could cause a single previously identified hazardous “top” event. Other (inductive) techniques such as FHA are more suitable for identifying a comprehensive set of system hazards. FTA is often used as a supplement to inductive techniques, in order to ensure control of severe hazards. Likely candidates for use of this technique include flight termination systems, systems that require dual fault tolerance, or command-and-control systems with stringent mishap risk requirements. This technique requires personnel with medium to high experience and

skill to perform well, and can be expensive. When judiciously applied, FTA can pay for itself many times over.

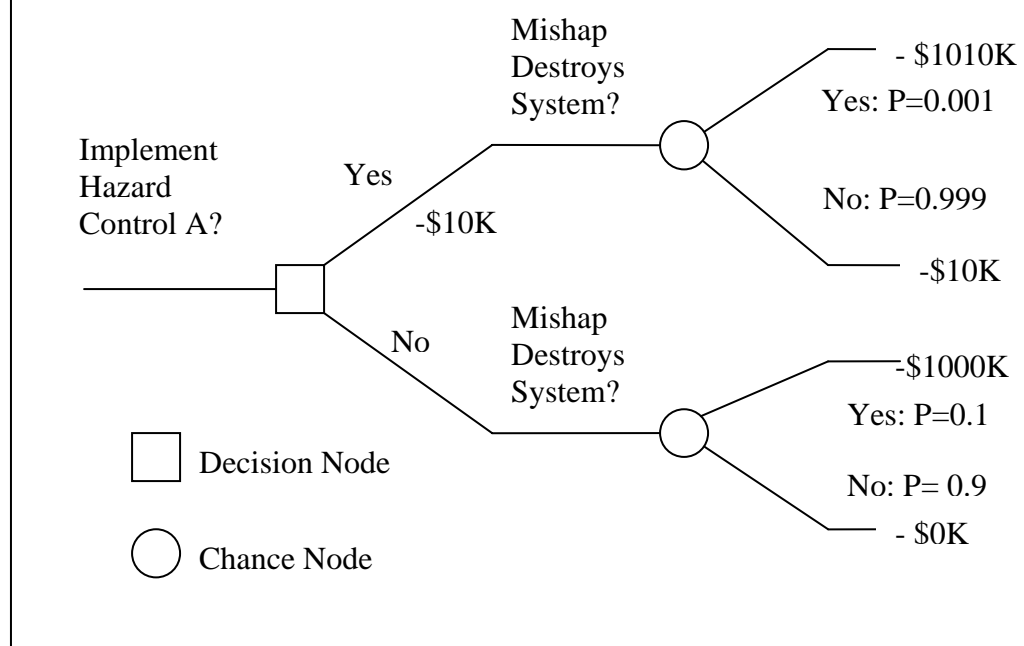
4.2.2.8 Event Tree Analysis (ETA)

Event Tree Analysis uses expected value to portray and explore all credible system operating outcomes. Severities, probabilities and costs are filled in during the course of event tree development. The SSE initiates the tree by drawing a single line, and then splits the line at various nodes representing possible chance events or decisions. Each line defines a possible outcome, such as success or failure. Each outcome may in turn initiate more lines which split off at other events or decisions, and in turn define other outcomes.

ETA differs from “fishbone” analysis in that it does not generally depict events, but instead depicts categories and sub-items chosen by the analyst.

When the event tree is finished, it depicts pathways from the single original initiating event to each anticipated potential final outcome. A value or penalty (such as severity of failure) is assigned to each final outcome, and probabilities assigned to each branch along the tree. If the values and probabilities are assigned throughout the tree in this manner, then expected values or risks of possible outcomes may then be calculated using a rollback procedure. When finished, the event tree depicts pathways from the single original initiating event, to each anticipated potential final outcome. Expected values or risks may also be calculated for various potential outcomes, events or management decisions pertaining to the system. Variations of event trees include success trees, fault trees, decision trees and cause-consequence analysis.

An example decision tree is shown in Figure 5.

FIGURE 5: EXAMPLE DECISION TREE

Results of an event tree are typically used in a subsystem or system hazard analysis. One limitation of the event tree is that the pathways and outcomes can only be those anticipated by the analyst. To ensure a comprehensive set of pathways or outcomes, team consultation or supplementary analyses such as history review are advisable. Another potential limitation is that if the event tree outcomes are expressed in terms of binary successes or failures, then partial successes or failures are not distinguishable. Some advantages of the event tree are that multiple failures can be analyzed, and that system weaknesses can be identified and prioritized for elimination.

4.2.2.9 Cause-Consequence Analysis (CCA)

Cause-Consequence Analysis explores time-sequenced system responses to initiating challenges, enabling probability assessments of success/failure outcomes, at staged increments. CCA is similar to ETA, but uses special symbols to describe conditions that may or may not exist, their consequences, and logical interrelationships.

The analyst may use the CCA at any point of the design. One typical use is to evaluate possible outcomes and derive strategies for emergency response and recovery. A limitation of the CCA (like Event Tree Analysis) is that the pathways and outcomes can only be those anticipated by the analyst. Advantages of the method include that multiple outcomes can be analyzed and that time sequences of events are treated.

4.2.2.10 Sneak Circuit Analysis (SCA)

A sneak circuit is an unexpected path or logic flow embedded in a system which, under certain conditions, can initiate an undesired function or inhibit a desired function. Sneak circuits are not the result of hardware failure but are latent conditions, inadvertently designed into the system and triggered by external inputs.

The four categories of sneak circuits are:

- ***Sneak paths*** which are unexpected paths along which current, energy, or logical sequence flows in an unintended direction;
- ***Sneak timing*** in which events occur in an unexpected or conflicting sequence;
- ***Sneak indications*** which are ambiguous, or false displays of system operating conditions that may cause the system or an operator to take an undesired action;
- ***Sneak labels*** which are incorrect or imprecise labeling of system functions may cause an operator to apply an incorrect stimulus to the system.

In order to analyze sneak circuits, the as-built system configuration is assessed compared to classical topographs. Key questions regarding each topographic element lead to discovery of sneak paths.

The SSE uses SCA to identify circuit design peculiarities that induce unwanted functions or inhibit wanted functions without component failures. Usually sneak circuit analysis is used in assessing system and O&SHA hazards. The advantage of using sneak circuit analysis is that the analysis provides insight into unintended circuit paths leading to potential system faults/failures. However applying SCA does not guarantee that all fault/failure paths can be found and the technique can be costly.

4.2.2.11 Bent Pin Analysis (BPA)

In Bent Pin Analysis, the SSE performs an evaluation of possible bent pin effects for one or more connectors, with special attention to safety critical functions. Bent pins may cause short circuits, a lack of continuity, or further mechanical damage, any of which might contribute to a mishap depending on the system.

To perform BPA the analyst needs to know connector pin locations, length, and proximity to adjacent pins and the surrounding casing. A BPA usually consists of three tasks:

- Identifying the system's critical functions;
- Determining the various permutations associated with each possible pin contact;
- Evaluating the potential effects and probability of occurrence.

The SSE considers the geometry of the connector, using software modeling and/or graphical methods. Some scoping assumptions shall be established, such as whether full bending and pin contact will occur if a pin starts slightly bent. Another assumption or ground rule is whether the analysis will address only pins carrying an identified critical

function, or all of the pins. Other assumptions to be considered are whether multiple pin bending or fault conditions other bent pins will be addressed. Selection of connector types can eliminate or greatly reduce the probability of failures. Common causes for bent pins include connector mismatching and direct pin probing with test probes.

Bent Pin Analysis can be applied at any time when proposed connector design and usage is known. This technique is typically applied on safety critical space and missile systems, conventional ordnance, nuclear weaponry or life support components.

Limitations of the technique are that it can be costly and time consuming if the scoping assumptions are broad or if the number of pins per connector is high. On the other hand, if the scoping assumptions are too narrow, significant failure effects and probabilities may be missed. BPA helps the SSE assure that a connector is safe to use in a given application, or to establish that a different design is preferable.

4.2.3 Mishap Risk Mitigation and Control

The system safety order of precedence is one of the most effective risk mitigations. The system safety order of precedence, in descending order of preferred technique, includes:

Design for Minimum Risk: The designer shall attempt to eliminate the risk. If risk elimination is not possible, the designer shall attempt to modify/change the design so as to reduce the value of the risk. Examples of these design modifications/changes include safety factors. A safety factor is the ratio of tensile or yield strength over the maximum allowable stress of the material or the ratio of burst pressure over the maximum allowable working pressure. Safety factors are used usually when a single point failure in the system structure would lead to a safety critical or catastrophic failure. For example, safety factors are usually used in structural design of high pressure containment systems and structural systems in satellites and rockets. Also, they are used in Ground Support Equipment (GSE) such as in hoists.

Incorporate Engineered Safety Features: If risk still remains after designing for minimum risk, the designer shall attempt to minimize the risk through engineered safety features. Examples of these features include active devices, i.e., redundant backups (fault tolerance), interlocks, and pressure relief valves. Provisions shall be made for periodic functional checks of the devices when applicable.

The fault tolerance method introduces redundant subsystems into the system to increase the probability that if one or more of the redundant subsystems failed the remaining redundant subsystem(s) would still function. As an example, for non-safety critical command and control functions; a system, subsystem, component, or subcomponent shall be designed in such a way that requires two or more independent human errors, or requires two or more independent failures, or a combination of independent failure and human error. For safety critical command and control functions; a system, subsystem, component, or subcomponent shall be designed that requires at least three independent

failures, or three human errors, or a combination of three independent failures and human errors.

Incorporate Safety Devices: If the mishap risk can't be designed out, and engineering safety features don't work, the designer shall try to mitigate the risk through the use of fixed, passive protective barriers (e.g. guards, shields, latches, and catches). Provisions shall be made for periodic functional checks of safety devices when applicable.

Provide Warning Devices: When design changes, engineered safety features, nor safety devices can adequately reduce risk, devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems. Examples of warning devices include chemical sniffers with alarm for high values of the harmful chemical, low oxygen level alarm, warning lights, and computer hazard monitoring & annunciation devices. These devices are of limited value for people with vision and hearing impairments.

Develop Procedures and Training: Where it is impractical to reduce risk to an acceptable level through design selection, with design changes, engineered safety features, safety devices, or warning devices, procedures and training shall be used. Procedures and training may include formal or informal training, checklists, certification or experience requirements, Personal Protective Equipment, etc. From MIL-STD-882C, without a specific waiver from the SPO, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for hazards with Category I or II severity. Precautionary notations shall be standardized as specified by the SPO, Tasks and activities judged to be safety critical by the SPO may require certification of personnel proficiency.

Frequently, combinations of the above techniques are used. For example, the designer could use engineered safety features, safety devices, and provide training for both of these methods.

4.2.4 Mishap Risk Verification

To ensure the mishap risk mitigations are acceptable for safety critical hardware, software, and procedures, the designer needs to verify the mishap risk mitigations. The verification methods include test, analysis, inspection, and simulation. Depending on the situation, these methods may be used alone or together. For example in some situations, testing and analysis may be the required verification methods.

4.2.4.1 Test

System and subsystem testing is typically the preferred method for mishap risk verification. SSPPs and test plans and procedure documents shall include these system verification tests. Testing usually gives the most accurate results of all the verification methods. However, this technique is costly, and utilization of testing may or may not be used, or combined with one of the other verification methods, such as analysis.

4.2.4.2 Analysis

Analysis is a mathematical model of the system/subsystem/component operation with the risk mitigation incorporated. Analysis is relatively inexpensive to conduct. Analysis can be used alone or in conjunction with each of the other verification methods. For example if proposed safety testing has a high or serious risk or is too expensive to perform, modeling or modeling in conjunction with a reduced amount of testing with a medium or low risk and low cost may be the technique of choice. The primary limitation of analysis, is that typically the model is simpler than the real world situation and therefore, may not give as accurate results as testing or analysis in conjunction with testing.

4.2.4.3 Inspection

While inspection is commonly used for quality and workmanship, as a verification technique inspection is the process in which the control, system/subsystem/ component, and the interface are carefully viewed to ensure they are built to the correct design. If the correct design build has not been accomplished, the system is reworked until the design build is accomplished. This method does not address the operation of the system/subsystem/component, control, and interface. However, by ensuring the as-built design is correct before testing, the method ensures that an incorrectly built system is not tested and used.

4.2.4.4 Simulation

Simulation is a verification technique which mimics the full scale testing of the system/subsystem/component with control. Simulation includes small scale (laboratory) testing, testing functional mockups, analogy (obtain the risk verification by examining this verification in similar systems), and computer simulation through the use of software models. Simulation tends to be less expensive than testing; however, the technique is of limited use as it will not give as accurate results of the design/operations safety of the system/subsystem/component of the system (including control) as testing or analysis in conjunction with testing.

4.3 System Safety in Operations and Testing

Ensure that the system can be safely tested and operated. Appropriate safety personnel shall review all operating plans, including test plans and perform hazard analysis to ensure that potential hazards are identified and their associated risks eliminated or otherwise controlled to acceptably safe levels. Identify facilities, equipment, requirements, specifications, documentation, procedural steps, training and criteria necessary to ensure and verify that the hazards are controlled. During operation or test execution, ensure safe performance of the operation or test.

Use the hazard tracking and mitigation risk resolution database to document hazardous conditions and systems deficiencies to enable the development of follow-on test or operational requirements for modified or new systems

4.3.1 Test System Safety

Hazardous systems and subsystems that are to be tested shall be tested safely, whether the tests are considered developmental or operational. In some cases the loss of a test item due to the test may be expected, and the loss of the test item may not be considered a mishap unless it represents an unexpected loss to the government. Test plans and objectives shall be considered in advance so that program and safety personnel will be able to identify and prevent potential mishaps and to appropriately react to a mishap should it occur.

4.3.1.1 Test Safety Review Board Process

The AFSPC/SMC Test Safety Review Board (TSRB) will be conducted IAW AFI 99-103 and supporting MAJCOM supplement. The TSRB provides an independent review of critical tests. SMC/SE shall be the final SMC authority for determining which tests are safety critical. The SPO TEMP and other test plans will identify safety critical tests based on the unique risks created by that test. The test safety review process is a tool that provides SMC risk acceptance authorities the information needed to evaluate the mishap prevention readiness of the test activity. The SPO and test personnel are urged to communicate test plans early to prevent undesired schedule impacts to the program, and to allow for TSRB planning, activities, deliberation, and possible test plan changes. Changes to the test plan after TSRB review will require re-coordination with the TSRB. The TSRB will occur before execution of the test. The TSRB shall be convened in a timely manner, considering proximity of the board to the beginning of the test and requirements to staff the test package. The test team may request the TSRB be combined with other review boards (e.g., technical and/or security review boards) to meet schedule objectives. TSRB membership shall include technically qualified system safety personnel who are organizationally independently from the test team or the organization executing the test activity. SMC/SE shall be the final SMC authority for determining who is technically qualified. Test plans for safety critical tests shall not be released without TSRB approval.

4.3.2 Operational and Space System Safety

Today's SMC SPOs act as Wings, with initial operational as well as developmental responsibilities. Also, since SMC's systems are almost always space systems or space-related systems, special safety requirements that apply to space systems shall be observed. SPOs shall ensure that proper safety tasks are planned, qualified people are provided to accomplish the tasks, authority is established and tasks implemented, and that sufficient resources (manning and funding) are provided to accomplish the tasks. Safety personnel participate in OSS&E processes such as Space Flight Worthiness Criteria development, Independent Readiness Review Team activities, and sometimes other special safety activities, in order that the system may safely become and remain operational.

4.3.2.1 Space Flight Worthiness Criteria

SPO safety and engineering personnel participate in the development of criteria, thresholds and targets for operational safety for their particular systems, with the assistance of SMC/SE representatives.

4.3.3 Operational and Space Safety Tasks

Operational and Space System Safety personnel help plan and execute tasks including list and schedule preparation of operational plans and procedures, operating instructions, technical manuals, safety training inputs, emergency and recovery procedures, mishap and anomaly reporting, corrective actions, continuous safety improvement, disposal or demilitarization, and collection and feedback of lessons learned into SPD and higher processes.

4.3.4 Corrective Actions

The corrective action process shall track hazards, list any needed corrective actions and establish corrective action priorities. The SSM/SSE is represented on change board with sign-off responsibility for items with potential system safety impact or those designated safety-critical. The SSM/SSE, following the guidance of SMC/SE, shall have the authority to determine what has system safety impact or is to be designated safety-critical.

4.3.5 Qualified People

Operational and space safety personnel shall meet qualification requirements that typically include training, and may include experience, certification, education or other requirements. Training requirements that may apply include weapons safety training,

space safety or orbital safety training. SMC/SE representatives assist in verifying qualification requirements and obtaining training.

4.3.5 Establishing authority

Operational and space system safety personnel assist management in establishing and maintaining authority for task accomplishment. Examples of authorizing documents that require safety input include SMC Instructions, SPO operating instructions, and program management guides or plans.

4.3.6 Resources

Operational and space system safety personnel assist management in obtaining resources, both manning and funding, to accomplish operational safety tasks. Manpower loading shall be planned for the program to allow for application of the appropriate amount of resources when they are needed. For example, participation of range safety personnel, operating wing Orbital Safety Officers or system safety engineers, customers, and warfighters/system users shall be planned, budgeted and obtained as required.

5.0 System Safety Relationship to Other Activities

Some types of systems and programs may require other activities such as interfaces with external safety organizations on a fairly regular basis. These activities include Nuclear Safety Activities, Department of Defense Explosives Safety Board, the USAF Non-Nuclear Munitions Safety Board, Air Transportation Logistics Agency, or operator/user/customer representatives. Applicability of these activities is generally describes in various DOD, USAF or AFSPC policies and instructions. SMC/SE representatives can assist program personnel in determining applicability of special activities or external reviews, and in interfacing with external organizations. Listed below are some of the more common activities.

5.1 Programmatic Environmental Safety and Health Evaluation

The Programmatic Environmental Safety and Health Evaluation (PESHE) is part of the Integrated Program Summary required by NSS-03-01 starting at Key Decision Point (KDP) B. At each KDP, the PESHE is updated. The PESHE should include, as a minimum, the following safety and health requirements:

- Strategy for integrating Environmental Safety and Occupational Health (ESOH), which includes system safety, Operations Safety and Health, Operational Safety, Suitability, and Effectiveness (OSS&E), and Explosive Safety;
- Identification of ESOH responsibilities for implementing this strategy;

- Identification of ESOH hazards to assess the risks, to mitigate or avoid those risks, to accept the residual risk, and to assess the effectiveness of the mitigations;
- Identification and status of ESOH risks (including the identification of hazardous materials used in the system and the plan for their demilitarization/disposal).

5.2 Operational Safety, Suitability, and Effectiveness

Air Force Policy Directive 63-12, Assurance of Operational Safety, Suitability, and Effectiveness, establishes the requirement to assure operational safety, suitability, and effectiveness (OSS&E) through a system's operational life. As such, it is the responsibility of the System Safety Manager to:

- Ensure mishap-reporting policies and procedures require an evaluation of system or end-item operational safety where system or end-item failures or deficiencies or failure to follow operational safety, suitability, and effectiveness processes are found to have contributed to the mishap.
- Ensure that appropriate System Safety policies and procedures are available for use in the acquisition process and for all systems and end-items.
- Ensure that mishap investigation information and recommendations are provided to the responsible Program Manager for a system or end-item involved in a mishap.
- Identify and communicate system and end-item safety hazards, risks, and recommendations to Program Managers and using commands for their assessment and action

5.3 SMC Independent Readiness Review Team (IRRT)

The SMC IRRT shall provide for participation of SMC/SE representatives, and the SPO shall provide resources as required for SMC/SE representative participation. SMC/SE participates on the SMC IRRT to provide independent System Safety Assessments of program activities, to ensure mishap prevention readiness and to share lessons learned. SMC/SE receives timely IRRT overview briefs, in-progress reviews such as MRR current risk assessments, consent to ship, available Aerospace Corporate President Reviews, Flight Readiness Review (FRR) formal risk assessments, and Post Flight Reviews.

5.4 Range Safety

Early and continuous coordination between the SSM, SMC/SE, and the Range Safety Office ("the Range", typically either the 30th SW/SE at Vandenberg AFB, or the 45th SW/SE at Patrick AFB) ensures that Launch Safety requirements are addressed early in the Program, and are key to a successful Launch and Mission partnership. Examples of such involvement include participation in the program reviews, SSGs/SSWGs, and review of safety documentation such as the MRAR and MSPSP. SMC Program Offices

shall obtain coordination or concurrence of safety documentation, to include any tailoring of such documents, with the applicable Range, and SMC/SE.

Range safety requirements are captured in EWR 127-1 (for legacy programs), AFSPCMAN 91-710, and AFSPCMAN 91-711 (descriptions of each can be found in the Appendix). Although these requirements are intended for Range Users and Operators, the SSM shall ensure that any items brought to the ranges by the SMC Wings to support launch operations also comply with Range Safety requirements.

Range Safety requirements from the above documents are tailored (i.e. deleted, altered, or added) to better accommodate the program being supported in a more efficient and economical manner. It is the responsibility of the System Wing to ensure that funding is made available in order to perform those both the tailoring activity and the proper execution of those tailored tasks. Tailoring of AFSPCMAN 91-710 (or EWR 127-1 for legacy programs) is conducted by the Contractor and/or the SSM, with the assistance of SMC/SE and the Range. Similarly, the tailoring for AFSPCMAN 91-711 is conducted by the SSM, with the assistance of SMC/SE and the Range. The Range reserves final approval authority for these tailored documents.

Range personnel, as well as their contractors, should be participants at the regularly scheduled System Safety Working Groups and System Safety Group meetings. Specific agenda topics that may be of interest to the Range include:

- Incidents, near-misses, and mishaps (to include Investigation and Root Causes), particularly those involving pre-launch, launch, and post-launch operations
- Flight Termination Systems
- Launch Vehicle and Upper-stage debris or disposal
- Controlled re-entry of launch vehicles, upper stages and spacecraft
- Explosives, Propellants, and Pressure Vessels

As part of the overall Program Offices Lessons Learned process, the SSM should capture and implement any lessons learned and design solutions recognized by the Ranges as an acceptable means of compliance.

5.5 Operational Risk Management

There is a direct relationship between system safety and risk management. All SMC organizations are required to have a risk management plan tailored to their mission and acquisition strategy. This risk management plan will be a valuable tool to the System Safety Manager and every effort should be made to leverage the strengths of both programs to ensure the greatest opportunity for mission success. There are several areas that a System Safety Manager should focus on with Operational Risk Management.

System Safety Managers (SSM):

- Should read, understand and be able to properly interpret and apply AFI 90-901 AFSPC Sup, AFPAM 90-902, and all applicable SMC and organizational risk management guidance. The organization's Risk Manager (RM) is the functional expert in this area and will provide a better understanding of both the AF's and the organization's tailored policies.
- Should meet and develop a working relationship with the organization's RM and his alternate to understand their roles in the program and how they are able to assist the SSM.
- Shall ensure that system safety issues, when identified and appropriate, are included in the Program Office's RM database.
- Should attend the scheduled risk management meetings and provide input to mitigation actions and risk rankings. SSM's shall provide guidance to the risk management team if and when necessary.

SSM's are always welcome to contact SMC/SEO to clarify any questions or assist in the Risk Management Process.

Appendix A: Major System Safety Products

A. 1 System Safety Management Plan

The Program/SPO SSMP describes system safety management and engineering tasks in the System Safety Program (SSP). While each program will be different, all SSMPs have the same general content. The following sample SSMP outline is provided as an aid in the effort to create the unique SPO SSMP. SMC/SES shall work with SPO personnel in drafting the SSMP by providing additional samples and writing support.

Government SPO System Safety Management Plan (SSMP) Outline:

TITLE PAGE

SIGNATURE PAGE

- Revision History

CONTENTS

CHAPTER 1 GENERAL

- SSP Scope, Purpose and Objectives
- Reference key documents including SMCI 63-1205, and separate SPO System Safety operating instructions or SSG charters if any. Reference appendices with terms, reference documents, mishap risk management procedures

CHAPTER 2 MANAGEMENT

- System Safety and SPO organization
- Personnel authority and responsibility including Military, Civil Service, FFRDC, SETA and contractor
- Interfaces with other organizations including SMC System Safety Staff
- Interfaces and integration with other SPO processes including Risk Management, PESHE, OSS&E/Mission Assurance and Systems Engineering to ensure all necessary tasks are accomplished and none duplicated
- SSM direct access to program manager
- SSM Functions in the SPO
 - SPO point of contact for System Safety activities and consultation of behalf of the SPD
 - SPO SSG, SSWG and Mishap Prevention/Risk Management
 - SSM/SSE Design Drawing Review and Approval
 - SSM membership in SPO processes including CCB
- Task, Data, Schedule and Resource Requirements

- Schedule, manning and funding policy for tasks and data for all SPO programs in various phases
- Tasks including acquisition strategy participation, RFP development, proposal evaluation and source selection, Task Order & Plans development for FFRDC support, obtaining SETA support, etc.
- Schedule
- Manning resources for SPO and programs including Military, Civil Service, FFRDC, SETA and contractor
- Funding
- Personnel Qualification Requirements (Education, Training, Experience, and Certification)

CHAPTER 3 SYSTEM SAFETY ENGINEERING

- Areas of emphasis for system safety efforts
- List analyses and data needed (i.e., PHL, PHA, SSHA, SHA, O&SHA, SSPP, MRAR, etc.)
- Require system safety personnel to review each ECP, hazard or mishap risk classification, accident and mishap or anomaly, corrective action suspense and corrective action. Specify ECP safety review sheet information.
- Specify that design review presentations will include system safety engineering impacts, and that concept and design proposals will not be accepted as complete unless they include safety impacts.
- Specify participation in SSG/SSWG activities by Military, Civil Service, FFRDC, SETA and Contractor personnel. (See appendix for SSG Charter).
- Schedule milestones and deadlines for system safety engineering tasks
- Draft schedule completion dates
- PHAs complete deadline, example 30 days before PDR
- SSHA complete deadline, example 30-45 days before CDR
- SHA complete deadline, example 30-45 days before CDR
- O&SHA complete deadline, example 60 days before test or operation
- Other...

CHAPTER 4 SAFETY VERIFICATION AND OPERATION

- Task safety engineering personnel to prepare and coordinate test plans and procedures
 - Test Safety and Test Safety Review Board
 - Safety Tests
- Operational and Space Safety
 - System Safety roles and responsibilities in SPO and Program OSS&E
 - Space Flight Worthiness Criteria
 - Independent Readiness Review Team
 - Plan operational and space safety tasks (list and schedule preparation of operational plans and procedures, operating instructions, technical manuals, safety training inputs, emergency and recovery procedures, mishap and anomaly reporting, corrective actions, continuous safety

improvement, collection and feedback of lessons learned into SPD and higher processes, ...)

- Provide requirements for qualified people to accomplish the tasks (Weapons Safety training, Space Safety training, Orbital Safety Officers, ...)
- Establish authority for implementing tasks through all levels
- Provide resources (manning and funding) to accomplish the tasks
- State requirements for getting the operational community (range safety officers, operating wing Orbital Safety Officers, customers and warfighters/system users) involved in the SPO programs' System Safety processes

CHAPTER 5 OTHER/SPECIAL TOPICS

- This chapter might include instructions for interfacing with external safety organizations that may be dealt with on a fairly regular basis such as Nuclear Safety Activities, Non-nuclear Munitions Safety Board, Air Transportation Logistics Agency, Range Safety or operator/user/customer organizations.

CHAPTER 6 APPENDICES (include here items that would require SPD approval or formal SSG action to change)

- SPO SSG Charter
 - SSG Objectives
 - Responsibilities
 - Meetings and Decision-Making
 - Support
 - Membership
 - System Safety Working Groups
 - Revision of Charter
- SPO Hazard/Mishap Risk Analysis Methodology, Criteria and Forms
- SPO System Safety Contracting Requirements and Recommendations

CHAPTER 7 ATTACHMENTS (include here items that could be updated by the SSM)

- List(s) of key personnel (by name)
- Safety status tracking charts
- Glossary of Terms and Acronyms
- SSMP References List
- SPO SSG and SSWG documents
 - Charter(s) or plans for continuous SSWGs (if any) such as those that may cover a particular program or long term effort in support of the SPO SSG
 - Charter(s) or plans for temporary or ad-hoc SSWGs such as may cover specific problems for specific times

A.2 Sample Language for Statement of Objectives

"Implement an environmental, system safety and health program from concept through disposal that is in accordance with Department of Defense, Air Force, and SMC policy directives and instructions, and also with federal, state, and local laws"

A.3 Sample Language for Statement of Work

"The Contractor shall develop and implement a preliminary System Safety Program Plan (SSPP) for the Program. Contractor shall implement and conduct a Phase A appropriate environmental, system safety and health program that supports the system life cycle from concept through disposal and that is compliant with federal, state, and local environmental, safety, and health laws and regulations and applicable Department of Defense, Air Force, and SMC policy directives and instructions.

"The contractor shall establish and implement a system safety engineering and management program in accordance with MIL-STD-882C (Tailored), shown below, and ..."

A.4 Preliminary Hazard Analysis Table

Subsystem/Operation: TT&C

Mission Phase: Pre-Launch Tests and Processing

Hazard Cause	Hazard Level/ Effect	Safety Requirements	Hazard Control	Verification	Status
1. RF emitters exceed allowable personnel limits for planned ground and pre-launch operations.	1. Critical – Personnel Injury	1. <i>EWB 127-1 Para. 3.8.1.1 a</i> Radio Frequency Emitters shall be designed to ensure that personnel are not exposed to hazard levels in excess of those specified in AFOSH 161-9	1. Testing and maintenance of RF emitters is accomplished only with antenna hats installed to attenuate the RF energy so that personnel are not exposed to average RF power density levels exceeding 10 mw/cm ² in accordance with AFOSH 161-9.	1. Review of drawings, RF hat attenuation analysis, test, and procedures.	1 . O p e n

A.5 Hazard Control Report

SMC/SES		HAZARD REPORT		Hazard Report Number: _____
System Safety Program		Date: _____		
FROM:	TO:	ACTION ADDRESSEES:		
SYSTEM:		COMPONENT:		
SYSTEM PHASE OR OPERATION:				
HAZARD DESCRIPTION (Outcome, mechanism and source)				
INVESTIGATION:				
SEVERITY: I II III IV		PROBABILITY: A B C D E		INITIAL RISK INDEX:
RECOMMENDED HAZARD CONTROL ACTION(S):				
RECOMMENDED VERIFICATIONS				
REFERENCE(S):		TELEPHONE:		
INDIVIDUAL IDENTIFYING SITUATION:				
FINAL RESOLUTION and RISK INDEX:	_____ HR REVIEW AUTHORITY (DATE)		USE ADDITIONAL SHEETS AS NECESSARY	
HAZARD RESOLVED & HR CLOSED:	PAGE 1 OF _____			
	RISK ACCEPTANCE AUTHORITY (DATE)			

A.6 Hazard Risk Acceptance

The Hazard Risk Assessment Matrix below contains hazard severity categories that are defined to provide a qualitative or quantitative measure of the worst credible mishap from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction. These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the SPO and the contractors as to the meaning of terms used in the category definitions. The adaptation shall define what constitutes system loss, major or minor system or environmental damage, and severe and minor injury and occupational illness.

The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports.

Hazard Assessment Matrix			Hazard Probability				
			Frequent	Probable	Occasional	Remote	Improbable
			A	B	C	D	E
SEVERITY	Catastrophic	I					
	Critical	II					
	Marginal	III					
	Negligible	IV					
			Risk Levels				

<u>Hazard Probability Definition</u>	
<i>Frequent</i>	Likely to occur frequently in life of system, item, facility, etc. Continuously experienced in fleet/ inventory. Probability of Occurrence: $(X) > 10^{-1}$
<i>Probable</i>	Will occur several times in life of item. Will occur frequently in fleet/inventory. Probability of Occurrence: $10^{-1} > (X) > 10^{-2}$
<i>Occasional</i>	Likely to occur sometime in life of item. Will occur several times in fleet/ inventory. Probability of Occurrence $10^{-2} > (X) > 10^{-3}$
<i>Remote</i>	Unlikely but possible to occur in the life of an item. Unlikely, but can reasonably be expected to occur in fleet or inventory. Probability of Occurrence $10^{-3} > (X) > 10^{-6}$
<i>Improbable</i>	So unlikely it can be assumed occurrence may not be experienced. Unlikely to occur, but possible in fleet or inventory. Probability of Occurrence $10^{-6} > (X)$
<u>Severity Definition</u>	
<i>Catastrophic</i>	Death or permanent total disability, system loss, major property damage, loss exceeding \$1M, or irreversible severe environmental damage that violates law or regulation.
<i>Critical</i>	Permanent partial disability or temporary total disability in excess of three months, major system damage, significant property damage Loss exceeding \$200K but less than \$1M, or reversible environmental damage causing a violation of law or regulation.
<i>Marginal</i>	Minor injury, lost workday accident, or compensable injury/illness; minor system or property damage, loss exceeding \$10K but less than \$200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
<i>Negligible</i>	First aid or minor supportive medical treatment, minor system impairment. Could result in injury or illness not resulting in a lost work day, loss less than \$10K, minimal environmental damage not exceeding law or regulation.

The next chart was created by SMC/SES to correspond to the SMC policy of assigning risk to the appropriate risk acceptance authority. It has a direct correlation to the Hazard Risk Assessment Matrix listed above for severity and probability risk.

Residual Hazard Risk Assessment Value	Hazard Risk Category	Hazard Risk Acceptance Level
IA, IB, IC, IIA, IIB	High	Milestone Decision Authority (PEO/MDA)
ID, IIC, IIIA, IIIB	Serious	Program Executive Officer (PEO)
IE, IID, IIE, IIIC, IIID, IIIE, IVA, IVB	Medium	Program Manager (PM)
IVC, IVD, IVE	Low	SSM/Chief Engineer Summary to PM

This chart is an example of the Hazard Risk Assessment Matrix from the NASA X40A Phase 2 acquisition program.

X40A Phase 2 Hazard Assessment Matrix		Hazard Probability				
		Frequent	Probable	Occasional	Remote	Improbable
		A	B	C	D	E
AX-04 Battery Rupture/Leakage	I				AX-10 IX-06	AX-04 AX-16
AX-10 Damage/Loss of X40A due to Flight Software Malfunction				GX-23		IX-25
AX-16 Loss/Damage of X40A due to landing gear/Tire Malfunction						
GX-23 Electrical shock to ground personnel						
IX-06 Premature/Off-nominal X40A release	II					
IX-25 Loss of X40A flight critical ground communications	III					
	IV					
		Status: 03 April 2000				

A.7 Example Tailored MIL-STD-882C Task Lists

A.7.1 Example Tailored MIL-STD-882C Task List: Satellite/Launch Vehicle

- Task 101 (System Safety Program). Comply with all of section 4. The qualification requirements of the SSM shall be based on table 3 for the program of high complexity. Acceptable level of risk shall be based on Figure 2. The resolution of residual risk shall be accomplished per the requirements of Figure 3. System safety shall be included in the WBS.
- Task 102 (SSPP). The SSPP shall be contractually binding when approved by the SPO.
- Task 103 (Integration of Associate Contractors, Subcontractors and A&E Firms). (Assume prime and sub contractors). Apply entire task except 103.2.1 and 103.2.2.
- Task 104 (System Safety Program Reviews). Contractor shall support all milestone reviews and audits.
- Task 105 (SSG/SSWG Support). The contractor shall be a technical advisor to the SSG. The contract shall support one SSG, a test review meeting and two other safety meetings per contract year. This support shall include briefing assigned topics at these meetings and answering questions related to the system safety effort.
- Task 106 (Hazard Tracking and Risk Resolution). The contractor shall maintain a hazard log of all hazards initially ranked as a Category I, II or III (Catastrophic, Critical or Marginal) severity. These hazards shall be included in the Data Accession List and be accessible to the government
- Task 107 (System Safety Progress Summary) Prepare quarterly system safety reports as part of the SPO Quarterly Review.
- Task 201 (PHL). The contractor shall begin preparing the list NLT shortly after KDP A. The list shall be completed by SRR.
- Task 202 (PHA). All.
- Task 203 (SR/CA). All.
- Task 204 (SHA). All.
- Task 205 (SSHA). All.
- Task 206 (O&SHA). All.
- Task 207(HHA). All (task will be discussed).
- Task 302 (Test and Evaluation Safety). The contractor shall comply with all range safety test requirements.
- Task 303 (Safety Review of ECPs, SCNs, SPRs, and Requests for Deviation/Waiver). The contractor SSM shall notify the SPO within one working day of identifying the change in the hazard severity or probability by one level.
- Task 401 (Safety Verification). Safety critical items shall include command and control elements of a system, subsystem or component; fuses, firing circuits, and safe and arm devices for ordnance; and any hardware, software or procedures that controls risk for catastrophic or critical severity hazards.

- Task 403 (EHC Data). Tailor 403.2.1 to include only the AF Explosive Hazard Classification Procedures. Delete 403.2.1.2.

A.7.2 Example Tailored MIL-STD-882C Task List: Ground System

- Task 101 (System Safety Program). Comply with all of section 4. The qualification requirements of the SSM shall be based on table 3 for the program of moderate complexity. Acceptable level of risk shall be based on Figure 2. The resolution of residual risk shall be accomplished per the requirements of Figure 3. System safety shall be included in the WBS.
- Task 102 (SSPP). The SSPP shall be contractually binding when approved by the SPO.
- Task 103 (Integration of Associate Contractors, Subcontractors and A&E Firms). (Assume prime and sub contractors). Apply entire task except 103.2.1 and 103.2.2.
- Task 104 (System Safety Program Reviews). Contractor shall support all milestone reviews and audits.
- Task 105 (SSG/SSWG Support). The contractor shall be a technical advisor to the SSG. The contract shall support one SSG, a test review meeting and two other safety meetings per contract year. This support shall include briefing assigned topics at these meetings and answering questions related to the system safety effort.
- Task 106 (Hazard Tracking and Risk Resolution). The contractor shall maintain a hazard log of all hazards initially ranked as a Category I, II or III (Catastrophic, Critical or Marginal) severity. These hazards shall be included in the Data Accession List and be accessible to the government
- Task 107 (System Safety Progress Summary) Prepare quarterly system safety reports as part of the SPO Quarterly Review.
- 200 Tasks - None
- Task 301 (Safety Assessment). All.
- Task 302 (Test and Evaluation Safety). The contractor testing shall conform to OSHA, State, and Local Safety regulations.
- Task 303 (Safety Review of ECPs, SCNs, SPRs, and Requests for Deviation/Waiver). The contractor SSM shall notify SPO within one working day of identifying the change in the hazard severity or probability by one level.
- Task 401(Safety Verification). All.

A.8 Contractor Data Requirements Lists (CDRLs)

Satellite/Launch Vehicle:

- System Safety Program Plan (information on 1423-1 form).
 - Block 2 System Safety Program Plan
 - Block 4 DI-SAFT-80100A
 - Blocks 10, 12, and 13. See Block 16
 - Block 16. Blocks 10, 12 & 13. Initial submission with bid. Final initial submission 30CD after contractor award. Updated preliminary versions shall be submitted 30CD prior to each IPA and each design review. Update final versions due 30CD after each IPA/design review.
 - Block 14. 1 copy to SMC/SPO SSM and 1 copy to SMC/SE
- Mishap Risk Assessment Report
 - Block 2. Mishap Risk Assessment Report/ Missile Systems Pre-launch Safety Package.
 - Block 4 DI-SAFT 81300A
 - Blocks 10, 12, and 13. See Block 16
 - Block 16. Preliminary submission 30CD prior to PDR, CDR and 90 CD prior to shipment . Final submissions 45 CD after PDR, CDR and 30CD prior to shipment.
 - Block 14. 1 copy to SMC/SPO SSM, 1 copy to SMC/SE(AXZ), and 1 copy to range safety.

Ground System

- System Safety Program Plan (information on 1423-1 form).
 - Block 2 System Safety Program Plan
 - Block 4 DI-SAFT-80100A
 - Blocks 10, 12, and 13. See Block 16
 - Block 16. Blocks 10, 12 & 13. Initial submission with bid. Final initial submission 30CD after contractor award. Updated preliminary versions shall be submitted 30CD prior to each IPA and each design review. Update final versions due 30CD after each IPA/design review.
 - Block 14. 1 copy to SMC/SPO SSM and 1 copy to SMC/SE (same as for satellite/launch vehicle program)
- SAR
 - Block 2 Safety Assessment Report.
 - Block 4 SI-SAFT-89182A
 - Blocks 10, 12, and 13. See Block 16
 - Block 16. Preliminary submission 30CD prior to PDR and CDR. Final submissions 30 CD after PDR and CDR.
 - Block 14. 1 copy to SMC/SPO SSM and 1 copy to SMC/SE.

A.9 Data Item Descriptions (DID) List and Accessible Data Products List (ADPL)

DID Number	DID Title
DI-H-1329A	Accident/Incident Report
DI-SAFT-80100A	System Safety Program Plan (SSPP)
DI-SAFT-80101A	System Safety Hazard Analysis Report
DI-SAFT-80102A	Safety Assessment Report
DI-SAFT-80103A	Engineering Change Proposal System Safety Report
DI-SAFT-80104A	Waiver or Deviation System Safety Report
DI-SAFT-80105A	System Safety Program Progress Report
DI-SAFT-80106A	Health Hazard Assessment Report
DI-MISC-80508	Technical Report - Study Services
DI-SAFT-80931	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-ADMN-81250	Conference Minutes
DI-SAFT-81299	Explosive Hazard Classification Data
DI-SAFT-81300	Mishap Risk Assessment Report
DI-ILSS-81495	Failure Mode, Effects, Criticality Analysis Report

A.10 DIDs and MIL-STD-882C Tasks Matrix

<i>DID No.</i>	<i>DID Description</i>	<i>Tasks Supported</i>
DI-SAFT-80100A	System Safety Program Plan	101 - System Safety Program 102 - System Safety Program Plan
DI-SAFT-80101A	System Safety Hazard Analysis Report	201 - Preliminary Hazard List 202 - Preliminary Hazard Analysis 203 - Safety Requirements/Criteria Analysis 204 - Subsystem Hazard Analysis 205 - System Hazard Analysis 206 - Operating and Support Hazard Analysis
DI-SAFT-80102A	Safety Assessment Report	301 - Safety Assessment 401 - Safety Verification 402 - Safety Compliance Assessment
DI-SAFT-80103A	Engineering Change Proposal System Safety Report	303 - Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/Waiver
DI-SAFT-80104A	Waiver of Deviation System Safety Report	303 - Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/Waiver
DI-SAFT-80105A	System Safety Program Progress Report	106 - Hazard Tracking and Risk Resolution 107 - System Safety Progress Summary 207 - Health Hazard Assessment
DI-SAFT-80931	Explosive Ordinance Disposal Data	404 - Explosive Ordinance Disposal Data
DI-SAFT-81299	Explosive Hazard Classification Data	403 - Explosive Hazard Classification and Characteristics Data
DI-SAFT-81300	Mishap Risk Assessment Report	Multiple Tasks

Appendix B: Acronyms

ACAT	Acquisition Category
ADPL	Accessible Data Products List
AFI	Air Force Instruction
AFPD	Air Force Policy Directive
AFOSH	Air Force Occupational Safety and Health
AFOTEC	Air Force Operational Test and Evaluation Center
AFSC	Air Force Safety Center
AFSPC	Air Force Space Command
AFSPCMAN	Air Force Space Command Manual
AoA	Analysis of Alternatives
APDP	Acquisition Professional Development Program
ARAR	Accident Risk Assessment Report
BS	Bachelor of Science degree
BPA	Bent Pin Analysis
CCA	Cause Consequence Analysis
CCB	Configuration Control Board
CDD	Capabilities Development Document
CDRL	Contract Data Requirements List
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CSOW	Contractor Statement of Work
CSP	Certified Safety Professional
CWBS	Contractor Work Breakdown Structure
DID	Data Item Description
DoD	Department of Defense
DoDI	DoD Instruction
DOT	Department of Transportation
ECB	Engineering Change Board
ECP	Engineering Change Proposal
EF/BA	Energy Flow/Barrier Analysis
ESOH	Environmental Safety and Occupational Health
ETA	Event Tree Analysis
EWR	Eastern and Western Range
FFRDC	Federally Funded Research and Development Corporation
FMEA	Failure Mode Effects and Criticality Analysis
FMECA	Failure Mode Effects Analysis

FAR	Federal Acquisition Regulation
FHA	Fault Hazard Analysis
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GSE	Ground Support Equipment
GPS	Global Positioning System
GSOW	Government Statement of Work
HAP	High Accident Potential
HHAR	Health hazard Assessment Report
HMMP	Hazardous Material Management Plan
HMMPP	Hazardous Material Management Program Plan
HMMPR	Hazardous Material Management Program Report
HQ	Headquarters
HR	Hazard Report
HRAM	Hazard Risk Assessment Matrix
H/W	Hardware
IAW	In Accordance With
ICD	Initial Capability Document, Interface Control Document
IG	Inspector General
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IOC	Initial Operating Capability
IPT	Integrated Process Team, integrated Product Team
IRRT	Independent Readiness Review Team
IT&E	Integration, Test, and Evaluation
JPO	Joint Program Office
JROC	Joint Requirements Oversight Council
JSC	Johnson Space Center NASA
KDP	Key Decision Point
LRR	Launch Readiness Review
MA	Managing Activity
MAJCOM	Major Command
MIL-STD	Military Standard
MRAM	Mishap Risk Assessment Matrix
MRAR	Mishap Risk Assessment Report
MRR	Mission Readiness Review
MS	Master of Science degree

MSPSP	Missile System Pre-Launch Safety Package
NAVEODTEHCEN	Naval Explosive Ordnance Disposal Technology Center
NDI	Non-Developmental Item
NSS	National Security Space
ORM	Operational Risk Management
O&SHA	Operating & Support Hazard Analysis
OSS&E	Operational Safety, Suitability, and Effectiveness
PDR	Preliminary Design Review
PESHE	Programmatic Environmental, Safety, & Health Evaluation
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager
PMR	Program Management Review
RF	Radio Frequency
RFP	Request for Proposal
SAR	Safety Assessment Report
SCA	Sneak Circuit Analysis
SCRA	Safety Requirements and Criteria Analysis
SDR	System Design Review
SEP	System Engineering Plan
SETA	Systems Engineering and Technical Assistance
SSHA	Sub System Hazard Analysis
SHA	System Hazard Analysis
SFW	Space Flight Worthiness
SM	Single Manager
SMC	Space and Missile Systems Center
SMC/EA	SMC Engineering and Architecture
SMCI	Space and Missile Systems Center Instruction
SMC/SE	SMC Safety Directorate
SMC/SES	SMC System Safety
SOO	Statement of Objectives
SOW	Statement of Work
SPD	System Program Director
SPO	System Program Office
SRD	Systems Requirements Document
SRR	System Requirements Review
SSE	System Safety Engineer
SSO	System Safety Officer

SSG	System Safety Group
SSHA	Subsystem Hazard Analysis
SSHAR	System Safety Hazard Analysis Report
SSM	System Safety Manager
SSMP	System Safety Management Plan
SSPP	System Safety Program Plan
SSPPR	System Safety Program Progress Report
SSWG	System Safety Working Group
S/W	Software
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TIM	Technical Interchange Meeting
TRD	Technical Requirements Document
TSRB	Test Safety Review Board
USD AT&L	Undersecretary of Defense for Acquisition, Technology, and logistics
WBS	Work Breakdown Structure

Appendix C: Applicable Documents

Document	Comments	Source
AF System Safety Handbook	This handbook provides an overview of System Safety	Air Force Safety Center, Kirtland, AFB
AFI 91-202 Air Force Mishap Prevention Program	SMC uses the AFSPC Supplement	http://www.e-publishing.af.mil/
AFI 91-204 Safety Investigations and Reports	SMC uses the AFSPC Supplement	http://www.e-publishing.af.mil/
AFSPCMAN 91-710 Range Safety User Requirements Manual	Superseded EWR 127-1. Used for new programs.	http://www.e-publishing.af.mil/
AFSPCMAN 91-711 Launch Safety Requirements for Air Force Space Command Organizations		http://www.e-publishing.af.mil/
AFMAN 91-222 Space Safety		http://www.e-publishing.af.mil/
EWR 127-1 Eastern and Western Range, 31 October, 1997	Used for legacy programs only.	
MIL-STD-882C System Safety Program Requirements	SMC Standard. Provides uniform requirements for developing and implementing a system safety program.	All versions can be found on the Web or from SMC/SE
National Security Space (NSS) Acquisition policy 03-01, 27 December 2004	Guidance for DoD Space System Acquisition Process	All versions can be found on the Web or from SMC/SE

Appendix D: Bibliography and Recommended Reading

- Ericson II, Clifton A. (2005). *Hazard analysis techniques for system safety*. Hoboken, NJ: John Wiley & Sons.
- McIntyre, Andy; Davis, Brett; Stringer, Brett; Liu, Eddie; Beasley, James; Wright, James; Sherman, Mike; Foster, Mollie; Kryska Paul; *Hazards analysis guide: a reference manual for analyzing safety hazards on semiconductor manufacturing equipment*, SEMATECH Technology Transfer document #99113846A-ENG.
- Moran, Ruben G. (2005). Bent pin analysis. *Proceedings of the 23rd International System Safety Conference*