BY ORDER OF THE COMMANDER
SPACE & MISSILE SYSTEMS CENTER

SPACE AND MISSILE SYSTEMS CENTER
INSTRUCTION 63-1205

28 JUNE 2011

Acquisition

THE SMC SYSTEM SAFETY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SMC/SES

Certified by: SMC/SES
(Mr. Thomas Meyers)
Pages: 85

This instruction implements AFPD 91-2. It consolidates system safety principles derived from DoDI 5000.02, DoDI 3100.12, AFI 91-202_AFSPCSUP1_I, AFI 91-217, AFI 63-101, AFI 63-1201, AFMAN 63-119, AFI 91-204_AFSPCSUP_I, AFMAN 91-222, AFI 91-103, AFSPCMAN 91-710 and MIL-STD-882C/D. It establishes SMC mishap prevention requirements, assigns responsibilities for program elements and contains system safety program management information required in system acquisition and Air Force safety directives, from concept through disposal. It applies throughout program life cycle of all SMC acquisition programs and projects (existing and future SMC space systems) that involve design, development, modification, evaluation, demonstration, testing, operation and disposal. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at https://www.my.af.mil/gcss-af61a/afrims/afrims/. This publication may not be supplemented. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, Recommendation for Change of Publication; route AF Form 847s from the field through the appropriate chain of command to SMC/SE, 483 N. Aviation Blvd., El Segundo, CA 90245-2808.

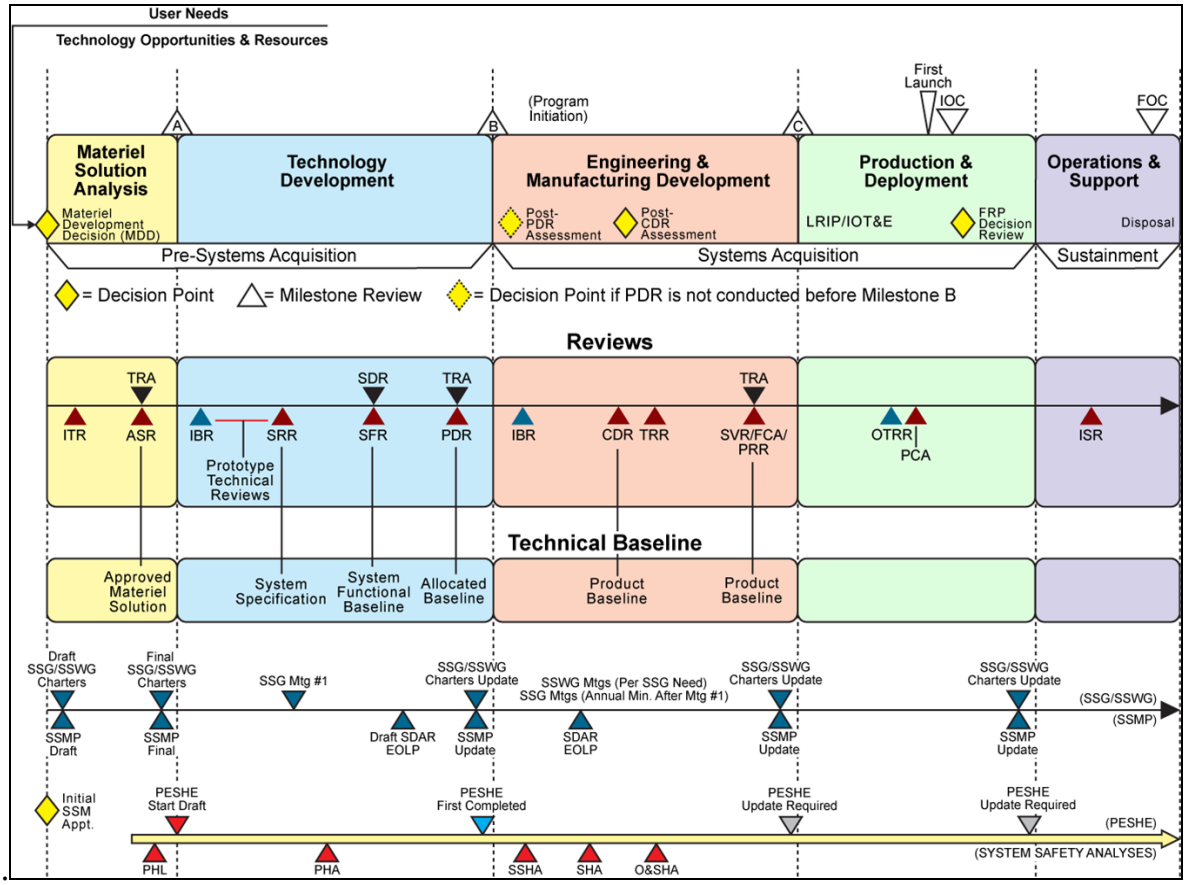
Chapter 1

PROGRAM OVERVIEW

1.1. Program System Safety. Program Managers (PM) or Product Support Managers (PSM), regardless of the Acquisition Category (ACAT) of their programs, are required to integrate system safety into their overall systems engineering and risk management processes (USD AT&L Letter, 23 Sep 2004). This document provides instruction in implementing the USD AT&L acquisition policy and it applies to all SMC acquisition programs and projects (existing and future SMC space systems) that involve design, development, modification, evaluation, demonstration, testing, operation and disposal. This instruction requires implementation of system safety requirements throughout the system life cycle to include Pre-Systems Acquisition, Systems Acquisition and Sustainment activities. Components of these activities include and correspond to defined scope of the Materiel Solution Analysis, Technology Development, Engineering & Manufacturing Development, Production & Deployment and Operations & Support phases of the program (see Figure 1.1 below). This instruction also requires implementation and maintenance of rigorous Operational Safety, Suitability and Effectiveness (OSS&E).

1.1.1. Figure 1.1 is based on DoDI 5000.02. It shows the life cycle of each space and missile system acquisition program (i.e., launch vehicle, spacecraft, ground control, and user equipment for which system safety requirements must be implemented). It aligns the system safety activities with other major system acquisition milestones. It covers the development of a solicitation, contract award, and management of the acquired system(s), from initial concept through the end of system life, including disposal.

Figure 1.1. Acquisition Phase /Flow Comparison



1.1.2. Contribution to mission success. Through systematic identification and control of the Systems Directorate's or Division's mishap risks, the system safety management, engineering and operational processes provide critical support to 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 capability, personnel injuries or human life, equipment damage, environmental contamination/damage, or ultimately the degradation or failure of the war-fighting mission and/or loss of combat personnel, systems and equipment.

1.1.3. Execution. 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. The SMC Engineering Directorate (SMC/EN), with assistance from the Directorate of Safety (SMC/SE) - creates and maintains, on behalf of the SMC Commander, the policy and guidance for SFW criteria. Each Program Office must tailor, build and maintain the SFW criteria for its own systems and program(s). The Program Office coordinates its SFW criteria with SMC/EN and SMC/SE representatives occasionally, such as when developing it or before milestone reviews, to seek advice. The Program Office formally coordinates the SFW criteria with SMC/EN and SMC/SE at least 30 days before presenting it before

SMC/CC or CD, as at the Flight Readiness Review/Operational Readiness Review (FRR/ORR).

1.1.4. System Safety Metrics. Metrics are applied to gauge the robustness of the Systems Directorates' system safety programs. SMC/SE generates the metrics as an independent evaluation and is provided to SMC/CC prior to SMC Program Management Reviews (PMRs). The metrics are generated to establish system safety goals and indicators of performance so satisfactory conduct of system safety at SMC can be measured throughout program life cycle.

1.1.5. Application of Requirements. As a significant contributing factor in the SMC mishap prevention program, every level of responsibility in the SMC acquisition activity shall implement SMCI 63-1205. Mishap prevention results from intelligent and systematic application of sound policies and trustworthy management and engineering skills. Mishap prevention also results from the degree of safety achieved in a given system, which is directly dependent upon the amount of management (government and contractor) emphasis.

1.1.5.1. Application of Requirements By Function. Commanders, functional managers, supervisors, and individuals must all contribute to the system safety mishap prevention program. An effective system safety program depends on individuals integrating mishap prevention at every organizational level and complying with applicable SMC safety policy and standards.

1.1.5.2. Application of Requirements In The Systems Directorate or Division. Systems Directorates must establish specific plans, instructions and procedures to ensure that all personnel and acquisition activities comply with SMCI 63-1205. Appropriate system safety verbiage must be included in key program documentation including the System Safety Management Plan (SSMP), Systems Engineering Plan (SEP), Test and Evaluation Management Plan (TEMP), Human Systems Integration Plan (HSIP), Cost Analysis Requirements Description (CARD) and in the Programmatic Environment, Safety and Occupational Health Evaluation (PESHE) document.

1.1.5.3. System Safety in Risk Management. System Safety must interface with Program Risk Management and must be represented in all key program elements including resources, processes and documentation. For example, system safety must be integrated in planning, cost analysis, configuration management, decision-making and record keeping activities.

1.1.5.4. Application of Requirements In Activities. SMCI 63-1205 requirements must also be applied on internal acquisition practices as well as on contracted activities. 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.

1.1.5.5. In Relationship to Other Technical Functions. The Systems Director, PM or PSM shall ensure that the system safety efforts are integrated across disciplines into systems engineering and other appropriate management and engineering disciplines as part of the Systems Directorate's total risk management process.

1.1.5.5.1. Mishap risk shall be an integral part of each management and engineering design task, each technical trade off study/decision, each test plan/test execution and operating procedure.

1.1.6. 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 external organizations include the Air Force Safety Center, Air Force Nuclear Weapons Center, Air Force Inspection Agency, Department of Defense Explosives Safety Board, the USAF Non-Nuclear Munitions Safety Board, Defense Logistics Agency, or operator/user/customer representatives. Applicability of these activities is generally described 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.

1.1.7. Available Support from SMC/SE. Each Systems Directorate will gain benefit from the aggregated experience of SMC/SE by requesting their support, attendance or participation in the Systems Directorate's acquisition activities. The Systems Director or PM or PSM must provide SMC/SE personnel access to Systems Directorate and contractor personnel, documentation, meetings and facilities to facilitate its support. In turn, SMC/SE will provide system safety expertise (provided manpower is available) to help define and resolve Systems Directorate's system safety issues.

1.1.8. System Safety Order of Precedence. Due to the complexity of space systems, it is impractical if not impossible to have them designed hazard-free. System safety precedence has been established for satisfying system safety requirements and reducing risks. As hazard analyses are performed, hazards will be identified that will require resolution. In selecting specific hazard controls, system safety engineers are generally guided by these "System Safety Order of Precedence." The order in which hazard controls are selected is as follows:

1.1.8.1. *Design for minimum risk* – Applied 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.

1.1.8.2. *Incorporate safety designs* – If an identified hazard cannot be eliminated or its associated risk cannot be 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.

1.1.8.3. *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.

1.1.8.4. *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.

1.1.9. Mishap Risk Condition. Positive action and implementation verification is required to reduce the risk due to unacceptable conditions to an acceptable level. The unacceptable and

acceptable mishap risk conditions or definitions described below are traditional and are appropriate for space systems.

1.1.9.1. *Unacceptable conditions* - The following safety critical conditions are considered unacceptable:

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

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

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

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

1.1.9.1.5. Hazard level categories that are specified as unacceptable in the contract or government effort.

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

1.1.9.2.1. For non-safety critical command and control functions, a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.

1.1.9.2.2. For safety critical command and control functions, a system design that requires at least three independent failures, or three human errors, or a combination of three independent failures and human errors.

1.1.9.2.3. System designs which positively prevent errors in assembly, installation, or conditions which could result in a mishap.

1.1.9.2.4. System designs which positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.

1.1.9.2.5. System design limitations on operation, interaction, or sequencing which preclude occurrence of a mishap.

1.1.9.2.6. 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.

1.1.9.2.7. System designs that control energy build-up which could potentially cause a mishap (Fuzes, relief valves, electrical explosion proofing, etc.).

1.1.9.2.8. System designs in which component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin.

1.1.9.2.9. System designs which positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been provided.

1.1.9.2.10. System designs which limit/control the use of hazardous materials.

1.1.9.3. Several higher level documents drive the use of fault tolerance in space systems (some identified below). Provide for meeting fault tolerance using:

1.1.9.3.1. AFSPCMAN 91-710, Volume 3, Section 3.2 (Systems Without Specific Design Criteria) requires dual fault tolerance for catastrophic, single for critical hazards.

1.1.9.3.2. AFI 91-217, Sections 3.3.10 (Safety catastrophic systems will be designed to be dual-fault tolerant for catastrophic hazards). The term "safety Catastrophic" implies a dual fault tolerance requirement per AFI 91-217.

1.1.9.3.3. AFI 91-217, Chapter 6, Section 6.4.4 (Warning systems have unique operational risks). The term "safety Catastrophic" implies a dual fault tolerance requirement per AFI 91-217.

1.1.9.3.4. Proven and Nationally accepted derivative requirement for risk reduction or order of precedence.

1.2. Risk Assessment and Management. System Safety and OSS&E will be identified as integral parts of a program's risk management effort integrated with the current SMC Operational Risk Management (ORM) Integration and Sustainment Plan. The scope of the assurance and preservation of OSS&E covers a significant portion of all of the program's risk.

1.2.1. The use of ORM-based system safety principles, tools, and techniques by all program office personnel are critical and will be used in assuring acceptable levels of risk throughout the life of the space or missile system.

1.2.2. A Systems Directorate's Risk Management Plan which defines the tasks to be performed by the government will be in place to assess the impacts of all program risks.

1.2.3. SMC programs will develop and implement system safety management and engineering processes and tools to sustain safety-related baseline capabilities during all modifications, upgrades, block changes, training, and other activities.

1.2.4. The system safety process will contain metrics that document how well the process is being employed with respect to the desired measurements of the system's space flight worthiness criteria.

1.3. System Safety in the Acquisition Cycle. The system safety process must provide the PM or PSM with the necessary information to allow for timely inputs into the integrated management framework at defined program milestones. With system safety analyses and other management tools, the system safety program will evaluate and document associated risks with identified hazards. The system safety activities for the program will involve early and timely participation and will be sustained throughout the life cycle. The earlier the system safety process can be started, implemented and accepted, the easier the system safety functions can be performed. Implementing the system safety process require thorough understanding of the logical systems engineering approach for obtaining system safety objectives. The System Safety Manager (SSM) is expected to master the process with guidance from SMC/SE.

Chapter 2

AUTHORITY, RESPONSIBILITY AND PROCESS

2.1. SMC/CC. makes policy and gives direction to ensure the timely application of system safety in SMC programs.

2.1.1. Directorate of Safety (SMC/SE). SMC/SE interprets and enforces SMC/CC system safety policy. SMC/SE evaluates the safety program of Systems Directorates or Divisions and provides advice to SMC/CC on system safety readiness of Air Force Program Executive Officer (AFPEO) programs.

2.1.1.1. System Safety Division (SMC/SES). SMC/SES will interpret and ensure system safety policy is applied across programs at SMC. SMC/SES must be the prime source of system safety expertise at SMC. SMC/SES engineers will be trained, experienced and will be fully qualified system safety experts in all aspects of system safety. SMC/SES engineers will have the authority and will be in a capacity to give technical advice to the program SSMs.

2.1.2. Systems Directorate or Division. The Systems Director or Program manager (PM) or Product Support Manager (PSM) must ensure that system safety engineering and management are integral parts of the systems engineering and management processes and will receive proper management attention. Depending on organizational structure, the Systems Director may occupy the same position as a Program Manager. At SMC, there may be Program Managers within a Systems Directorate or Systems Division. Also, per DTM-10-015, 07 October 2010,"..CAEs shall identify and assign a PSM within every ACAT I and ACAT II program, prior to but no later than program initiation." Therefore, the Systems Director, Program Manager and Product Support Manager are management entities in the Systems Directorate/Division.

2.1.2.1. The Systems Director or PM or PSM must also provide direct lines of communication to their system safety staff (primarily the SSM) to receive timely information on identified hazards that have high mishap potential.

2.1.2.2. System Safety Managers (SSM). SSMs shall manage the implementation of the system safety program at the Systems Directorate or Division. SSMs shall be trained and experienced and authorized to be in the capacity to perform the duties of a SSM in accordance with this SMCI. Unless otherwise stated, SSM throughout this SMCI refers to the government appointed person to manage the Systems Directorate's system safety program (see paragraph 2.1.2.3 below).

2.1.2.3. Systems Directorate or Division System Safety Manager (SSM) Appointment. The Systems Director or Program Manager or Product Support Manager shall appoint by letter a qualified System Safety Manager (SSM) to clearly define and document risk acceptance authority and execution during life-cycle system decisions. Additional information on the SSM's functional role and responsibility are discussed in Chapter 4.

2.2. System Safety Process.

2.2.1. Safety Program Management. Program management must ensure that safety offices monitor program requirements to identify and correct hazards throughout the operational life

of a system or facility to ascertain hazards are identified through operational experience, mission changes, environmental effects, or system modification.

2.2.1.1. Management must also ensure that safety staffs identify and control all hazards associated with decommissioning or disposal of a system.

2.2.2. Staff Support. Expertise from SMC/SE should be sought to adequately scope the required system safety effort to include the size and content of the SSMP. SMC/SE can help out in providing guidance in generating qualified and abbreviated system safety documentation.

2.2.3. System Safety Assessment of Programs and Criteria. To support the SMC/CC PMRs, SMC/SE submits system safety metrics against the Systems Directorates/Divisions.

2.2.3.1. Criteria used will include the quality and availability of the Systems Directorate's SSMP, System Safety Program Plan (SSPP), Hazard Tracking Tools, qualification of their SSM, the quality and frequency of their System Safety Group activity, and the robustness of their system safety program as verified and validated by the system safety activities described in their PESHE.

2.2.4. Safety Risk Management. The Program Manager (with support from their safety office and contractor and in consultation with SMC/SE) must clearly define and document risk acceptance authority during life-cycle system decisions as defined by MIL-STD-882.

2.2.4.1. Safety risk management identification, resolution, mitigation/elimination, disposition and documentation must be applied in a timely manner and integrally linked with the acquisition activities delineated in DODI 5000.02, AFI 63-101, AFI 63-1201, AFI 91-202_AFSPCSUP_I and this SMCI.

2.2.5. Environment, Safety and Occupational Health (ESOH). The PM or PSM shall ensure that appropriate ESOH efforts are integrated across disciplines and into systems engineering to determine system design characteristics that can minimize system, environment and personnel risks. System effects may include subsystem and/or component malfunction leading to mission failure. System risk reduction may include systems and operations design to enhance reliability and safety to promote mission success. Personnel effects may involve acute or chronic illness, disability, or death or injury to operators and maintainers; and enhancement of job performance and productivity of personnel who operate, maintain, or support the system.

2.2.5.1. The PM or PSM shall apply system safety per MIL-STD-882 in the risk reduction process, eliminate ESOH hazards where possible and manage ESOH risks where hazards cannot be eliminated.

2.2.6. Risk Acceptance. PMs or PSMs shall ensure that the status of ESOH risks and acceptance decisions is briefed at technical reviews and milestone reviews. The information provided at the technical reviews can be used as reference by interested technical disciplines to align/re-align program activities or disposition affected by system safety.

2.2.6.1. Acquisition program reviews and fielding decisions must address the status of all high and serious risks, and applicable ESOH technology requirements.

2.2.6.2. Prior to exposing people, equipment, or the environment to known system-related ESOH hazards, the PM or PSM shall document that the associated risks have been

accepted by the following acceptance authorities: the Service Acquisition Executive (SAE) for high risks, PEO-level for serious risks, and the PM or PSM for medium and low risks. SAE for space programs and for non-space programs is the Assistant Secretary of the Air Force for Acquisition (SAF/AQ). Notify through SAF/US and SAF/AQS.

2.2.6.3. SMC personnel shall ensure that the user representative will be part of this process throughout the life cycle, and shall obtain formal concurrence from the user prior to all serious and high-risk acceptance decisions. Users will vary from program to program but will generally include 14th AF/SE. AFI 91-217 noncompliances are sent to 14th AF/CC by SMC/CC.

2.2.7. Risk Acceptance Coordination. Serious and High risk acceptance packages will be coordinated with the user representative, SAF/AQR, and AF/SE before submission to the SAE for acceptance.

2.2.7.1. Program offices will coordinate risk acceptance packages with their local safety offices, SMC/SE and HQ AFSPC/SE. For space acquisitions, program offices will provide SMC/SE, IAW program phase, a list of preliminary and subsequent system hazards, mitigation measures, risk assessments, and risk acceptances. Certain risk packages must be sent higher for approval, e.g. those involving noncompliance with DOD directives and instructions, or with national space policy. Procedural guidance is evolving, particularly for launch and orbital systems casualty Expectation, End-of Life, debris minimization and collision avoidance requirements and waivers. Check with SMC/ENC (SMC Enterprise Compliance Engineering Division) and SMC/SE representatives for current information.

2.2.8. Test Risk Acceptance/Transfer. The PM or PSM, in concert with the user and the T&E community, will provide safety releases (to include formal ESOH risk acceptance) to the developmental and operational testers prior to any test that involves personnel exposure.

2.2.9. System Safety Management Plan (SSMP). Program management will ensure that a government System Safety Management Plan (SSMP) is generated and its requirements flowed down to their contractor's System Safety Program Plan (SSPP) and accomplished for all programs and projects including temporary and permanent modifications.

2.2.9.1. The SSMP requirement will apply to space product centers, laboratories, and systems directorates/divisions and is applicable to all programs, projects, development or modification to be evaluated, assessed, or tested, regardless of acquisition category and cost.

2.2.9.2. Program management must ensure that safety staff and other appropriate personnel monitor program requirements to identify and correct hazards throughout the total life of the system or facility.

2.2.9.3. Program Office personnel with System Safety responsibilities will ensure that safety criteria, hazard identification, resolution and disposition for all in-house and contractual programs are documented.

2.2.10. Programmatic ESOH Evaluation (PESHE). DoDI 5000.02 requires the PM or PSM, regardless of program ACAT level to prepare a PESHE which incorporates the MIL-STD-882D process and requires certain content. Other policies such as AFI 63-101 require additional content, and a future SMCI specific to PESHE is planned. Consult SMC/ENC,

SMC/SES and SMC/SEO for current comprehensive environmental, safety and health instructions and advice. A summary of the required PESHE content, which the SSM is expected to participate in developing, follows:

2.2.10.1. Identification of ESOH responsibilities.

2.2.10.2. Strategy for including ESOH considerations into the systems engineering process.

2.2.10.3. Identification of ESOH risks and their status.

2.2.10.4. Description of the method for tracking hazards throughout the life cycle of the system.

2.2.10.5. Identification of hazardous materials, wastes, and pollutants associated with the system and plans for their minimization and/or safe disposal.

2.2.11. SSMP and PESHE Schedules. The PESHE is required to support milestone decisions (MS) with an initial submittal at MS-B and updated at MS-C and Full-Rate Production (or Full Deployment) Decision Review (DR). Adequate lead time will be considered when contracting out data deliverables required as data source for the PESHE. The PESHE document must be coordinated by SMC/SE and SMC/EN, signed by the Systems Director and approved by the appropriate management authority prior to the MS decision it supports. The SSMP and PESHE program schedules and activities will correspond and/or complement each other.

2.2.12. DoDI 5000.02 also states that the Acquisition Strategy shall incorporate a summary of the PESHE. If personnel support from SMC/SES is available, the SSM (or PM or PSM) may request assistance from SMC/SES when generating system safety sections of the PESHE.

2.2.13. Demilitarization and Disposal. The approach for integrating safety considerations into the Demilitarization and Disposal planning process shall be delineated in the SSMP. At the end of its useful life, a system shall be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety (including explosives safety), security, and the environment. Disposal shall take into consideration space debris and public safety risk minimization or elimination. During the design process, PMs or PSMs must, with SSM assistance, document (in the PESHE) hazardous materials contained in the system and shall estimate and plan for the system's demilitarization and safe disposal.

2.2.14. Mishap Investigation Support. PMs or PSMs shall support system-related Class A and B mishap investigations (and other classes of safety investigations as appropriate) by providing analyses of hazards that contributed to the mishap and recommendations for materiel risk mitigation measures, especially those that minimize human errors. Mishap and event classifications and categories are discussed in AFI 91-204_AFSPCSUP1 and AFMAN 91-222.

2.2.15. Deficiency Reporting, Investigation, And Resolution. PMs or PSMs must ensure that their System Safety Managers (SSMs) are fully trained and qualified to effectively implement and participate in the USAF Deficiency Reporting and Investigating System (DRIS). This system promotes the ability to identify and correct deficiencies before they

impact mission capability; thus, promoting Operational Safety, Suitability and Effectiveness (OSS&E).

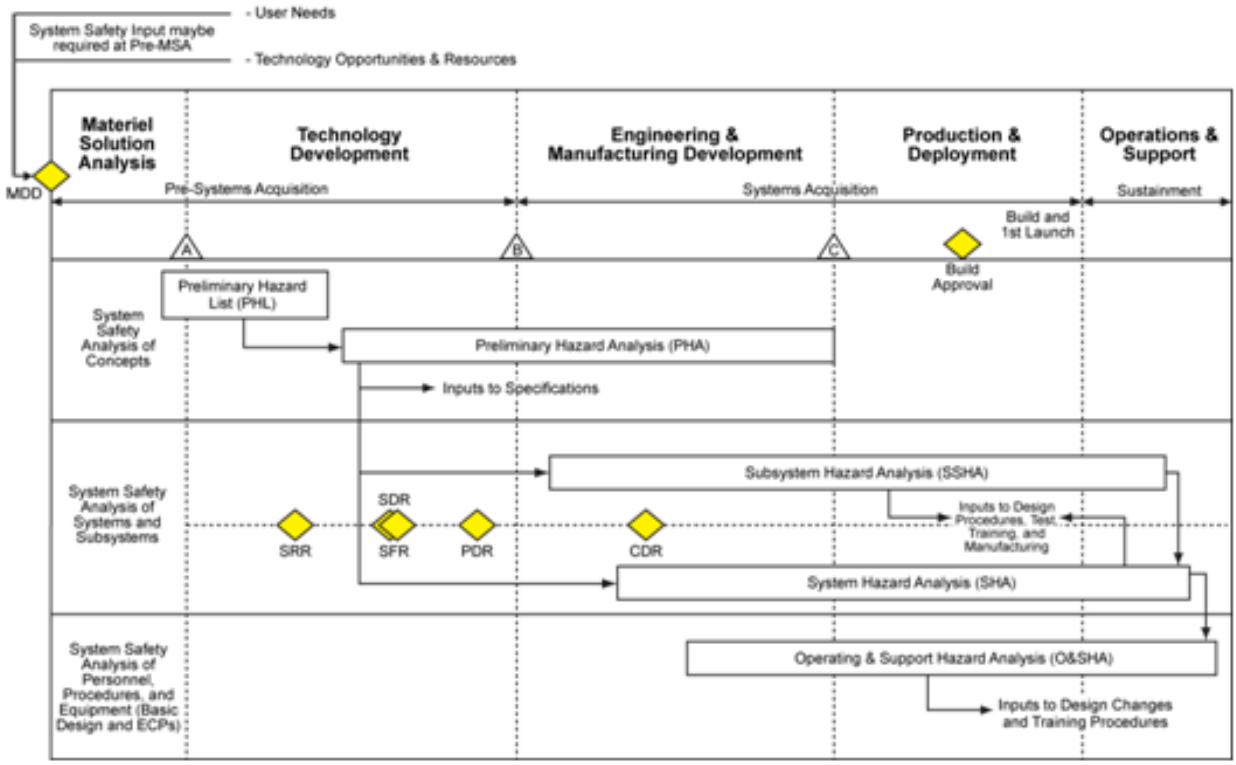
Chapter 3

SYSTEM SAFETY IN SMC SYSTEMS AND PROGRAMS LIFE CYCLE

3.1. System Safety in SMC Programs. System Safety will be implemented in Pre-Systems Acquisition, Systems Acquisition and Sustainment activities. Pre-Systems Acquisition covers activities from both Materiel Solution Analysis (MSA) and Technology Development (TD) program phases. Systems Acquisition covers activities from both Engineering & Manufacturing Development (EMD) and Production & Deployment (P&D) program phases. Sustainment covers activities in the Operations & Support (O&S) program phase and includes disposal. At the onset of the program cycle, the SSM will participate 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 suitable materials to use. The SSM may consult with SMC/SES for assistance.

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

Figure 3.1. Hazard Analysis Time Phased Relationships



3.1.1. System Safety is applicable throughout the entire System and Program life cycle, and is applied to mishap prevention and mishap risk management at all system levels. Potential losses to the government and reportable mishaps to be prevented may include those occurring pre-range/launch (e.g. losses at contractor facilities or during transportation), range/launch, or during the on-orbit phase (e.g. orbital safety mishaps and others). Hazards that are not readily apparent at one system level (e.g. personnel hazards for an unmanned space vehicle)

may exist at a different system level. Consult relevant guidance for mishap definitions including AFI 91-202 AFSPC SUP 1, AFI 91-204, AFI 91-217, and AFSPCMAN 91-710, and seek advice from SMC/SES personnel to aid in identification of hazards and potential mishaps. For example an on-orbit phase hazard analysis is required for systems that will include an on-orbit asset (See Section 5 for details).

3.2. Pre-Materiel Solution Analysis (Pre-MSA). Systems Directorates/Divisions will consider system safety input even at the Pre-MSA activities. Systems Directorates may also request input from SMC/SES for Pre-MSA activities and documentation to validate system safety need and ensure provision of adequate system safety coverage and strategy. Input may be provided at acquisition strategy meetings and/or review/comment to generated draft Acquisition Strategy Document (ASD).

3.2.1. System Safety input to pre-contract documents to support Pre-MSA efforts such as the Request for Proposal (RFP) or Request for Quotation (RFQ) will also be provided by the Systems Directorate/Division, Group or Program System Safety Managers (SSMs). System Safety input will also be provided by SSMs or equivalent from Staff Directorates or other SMC organizations with projects or programs that involve design, development, modification, evaluation, demonstration, testing, operation and disposal. Available support may be requested from SMC/SES. Typically, studies done for the Pre-MSA phase are contracted out and usually are technical capability studies. Identification of current and/or future system safety requirements may be required.

3.2.2. Initial Capabilities Document (ICD) and Materiel Decision Development (MDD). The System Safety Manager (SSM) will provide input to the Pre-MSA activities and documentation including development of the ICD to support the MDD process.

3.3. Pre-Systems Acquisition (MSA through TD). The SSM must be familiar with the activities and documentation generated in Pre-Systems Acquisition.

3.3.1. ICD, AoA and ADM. At the MSA phase, the SSM must be familiar with the ICD, Analysis of Alternatives (AoA) and Acquisition Decision Memorandum (ADM) as the information provided by these documents is necessary in evaluating and scoping the extent of the required system safety program. Other personnel including the PM must facilitate the SSMs access to these documents. The ACAT is usually provided by the ADM.

3.3.2. System Safety Management Plan (SSMP) and Preliminary Hazards List (PHL). At the MSA phase, the SSM (in consultation with SMC/SE) generates the draft SSMP. The SSMP shall be approved for implementation at MS-A approval or at the beginning of the TD phase. If the MSA effort is contracted out, the SSM should ensure that the PHL is a required data submittal; however, the System Directorate may opt to generate the PHL. A preliminary System Safety Program Plan (SSPP) should also be a data submittal that accompanies the PHL.

3.3.2.1. The SSM must define and develop mishap probability and severity level definitions for incorporation in the SSMP and application in the PHL and other system safety risk management documentation. The SSM will ensure that the SSMP and the SSPP are generated/updated and implemented throughout all phases of the program's life cycle.

3.3.2.2. Requirements from the SSMP must flow down to the SSPP and both documents will map the system safety process to the 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.

3.3.3. To support the Milestone-A (MS-A) approval process, the SSM will provide system safety input to key documents including the following program documentation to be submitted at MS-A (updates required at MS-B and MS-C):

3.3.3.1. Systems Engineering Plan (SEP). The SSM will provide system safety verbiage to the SEP ensuring the PM's or PSM's commitment to integrate Environment, Safety and Occupational Health (ESOH) risk management into the overall systems engineering process for all developmental and sustainment engineering activities.

3.3.3.2. Technology Development Strategy (TDS). The SSM will provide system safety verbiage to the TDS document. The TDS document describes at a minimum Commercial Off-The-Shelf (COTS) usage, the preliminary acquisition strategy to include cost schedule and performance goals for the development phase.

3.3.3.3. Test and Evaluation Strategy (TES). The SSM will provide system safety verbiage to the TES document. Test planning addresses the T&E process of competitive prototyping, early demonstration of technologies and the development of an integrated test approach.

3.3.4. Clinger-Cohen Act (CCA). The TD phase begins at MS-A approval and the SSM must be familiar with the CCA compliance requirements (statutory)(Ref. DoDI 5000.02 Enclosure 5). The SSM must also be familiar with and should provide input to the documentation required by the CCA. The documentation includes the Initial Capabilities Document (ICD), Capabilities Development Document (CDD), Capabilities Production Document (CPD), Acquisition Program Baseline (APB) and the Analysis of Alternatives (AoA). The effectiveness and extent of the system safety program depend heavily on the SSM's input to the CCA requirements and documentation. Program management's activities place a great deal of emphasis on the CCA requirements.

3.3.5. At the start of the TD phase, the SSM should have the SSMP approved by the Systems Directorate and the SSMP requirements will flow down to the following draft documents for support of MS-B approval:

3.3.5.1. Cost Analysis Requirements Description (CARD). The SSM will provide system safety verbiage to the CARD. Identified system safety requirements (to include resources, documentation, processes) and activities will provide information for budget projection necessary for the program throughout life cycle.

3.3.5.2. Programmatic ESOH Evaluation (PESHE). The SSM shall ensure that system safety requirements are adequately addressed in the PESHE documentation and related activities.

3.3.5.2.1. The SSM will ensure that the SSMP identified requirements and activities are reflected and complementarily evaluated in the PESHE process.

3.3.5.3. Test & Evaluation Management Plan (TEMP). The SSM will provide input to the TEMP (required at MS-B and updated at MS-C and Full-Rate Production decision).

The TEMP describes planned developmental, operational and live-fire testing including system performance evaluation.

3.3.5.4. Human Systems Integration Plan (HSIP). The SSM will ensure that the PM's or PSM's appropriate system safety requirements and activities are integrated in the HSI process.

3.3.6. Other Activities In Pre-Systems Acquisition. As a major part of the System Safety process, the SSM will participate in pre-contract activities such as preparing request for proposal objectives and source selection criteria as well as post-award surveillance of contractor activities including the events depicted in the Integrated Master Plan/Integrated Master Schedule (IMP/IMS) and the SSMP and SSPP.

3.3.6.1. Generally, SMC contracts out major acquisitions and the SSM must be intimately familiar with the activities and processes impacting system safety in the different acquisition phases including this phase. The acquisition system safety requirements, activities and processes should be documented in the SSMP and flowed down to the SSPP and IMP/IMS.

3.3.6.2. Request For Proposal (RFP) Input. In pre-contract activities, the SSM will ensure that system safety verbiage and data submittal required in pre-systems acquisition are reflected in the RFP package to include contents of the Government Statement of Work (GSOW), Contract Data Requirements Lists (CDRLs) and Sections L and M.

3.3.6.2.1. The SSM will ensure that the CDRLs include the System Safety Program Plan (SSPP), Preliminary Hazard List (PHL) and Preliminary Hazard Analysis (PHA). If the SSPP and PHL were CDRLs in a previous contract, then updates are required in this phase. Generally, system safety CDRLs may or may not be required at the Pre-MSA phase. At Pre-MSA, the major activities include studies or projects defining low level technology solutions to support the Materiel Development Decision (MDD). The SSM must analyze the effort to ensure that system safety is not compromised. SMC/SES assistance may be requested to help define the system safety requirements. The Pre-MSA activity has not yet entered the formal acquisition process. MDD approval begins MSA activities and Pre-Systems Acquisition and starts the formal acquisition process.

3.3.6.2.2. The SSM will provide input to the Offeror's instruction in the RFP that includes how system safety will be addressed in program management and systems engineering program execution. Input to the instruction will also require inclusion of narratives addressing event-driven tasks and products through the IMP/IMS and CWBS. System safety representation on engineering and management review boards will be required. The SSM will also be evaluating the Offeror's process in planning for system disposal (both for on-orbit and ground based systems), demilitarization, and end-of-life requirements.

3.3.6.2.3. The PM or PSM should consider assigning the SSM to participate in the source selection process. Participation of the SSM is important since he/she should be the most knowledgeable person in the Systems Directorate concerning program system safety. System safety criteria for the source selection must reflect instructions addressed in the RFP.

3.3.6.2.4. In the TD phase, the PM or PSM will ensure that adequate resources be provided to support the SSM function. Typically for the TD phase contract, more than one contractor are selected and one will be downselected for the EMD phase. In this circumstance, the workload for the appointed SSM may be more than doubled.

3.3.6.2.5. Data Submittal Review/Approval, TD Phase. As part of the contract management for system safety in this phase, the SSM will be involved in the review and approval of data submittals that include the SSPP, PHL, PHA and draft Space Debris Assessment Report (SDAR) to support PDR. The SSM must also get involved in the review and approval of other system documentation linked to systems engineering (specifications, analyses, trade-off studies, test, etc.), configuration management, reliability & maintainability, human systems integration, environmental management & engineering and risk management. All these documents influence system safety.

3.3.6.2.6. The SSM will also participate in requirements development and trade studies occurring at the TD phase.

3.3.6.2.7. The SSM will draft the language for contract solicitation that requires the Contractor's system safety effort to comply with the Government's system safety program.

3.3.6.2.8. In order to implement a comprehensive system safety program, other Pre-Systems Acquisition activities will also be accomplished to complement pre-contract and contract related activities. These activities include the following:

3.3.6.2.8.1. System Safety Group (SSG) and System Safety Working Group (SSWG). Ideally, early in Pre-Systems Acquisition, the SSM should ensure that the charter for the System Safety Group (SSG) is drafted, coordinated, finalized and approved for implementation. The SSM should also ensure that appropriate membership and activities are cited in the charter. The SSG should assist the SSM to provide additional expertise in the establishment of necessary requirements, criteria and documentation, especially for complex programs where a SSM could be overwhelmed. The SSG and SSWG are further discussed in Chapter 4 of this instruction.

3.3.6.2.8.2. The SSG will provide assistance to the Systems Directorate/Division concerning establishment 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.

3.3.6.2.9. The PM or PSM will ensure that an initial SSG meeting will take place at the early stages of the TD phase. The PM or PSM must ensure that at least one annual SSG meeting, at a minimum, will subsequently occur after the initial meeting.

3.3.6.2.10. In the Pre-Systems Acquisition Phase, the SSM will also participate in the technical and management reviews established by both the government and contractor. These reviews have attributes (cost, workbreakdown structure, schedules, system functions/specifications, risk resolutions, etc.) affecting system safety and they include the following:

3.3.6.2.10.1. Initial Technical Review (ITR).

3.3.6.2.10.2. Alternative Systems Review (ASR) and Technical Readiness Assessment (TRA). Both are related to established materiel solutions.

3.3.6.2.10.3. Integrated Baseline Review (IBR). The IBR is related to the Performance Measurement Baseline (PMB) and has direct link to the Work Breakdown Structure (WBS).

3.3.6.2.10.4. Prototype Technical Review (if needed to conduct for risk reduction of programs with relatively higher degrees of technical uncertainty).

3.3.6.2.10.5. System Requirements Review (SRR).

3.3.6.2.10.6. System Functional Review (SFR).

3.3.6.2.10.7. Preliminary Design Review (PDR).

3.3.7. The SSM and PM will also implement a system safety portion of the Acquisition Strategy using a SMC/SES developed template. For assistance, the PM or the PSM or the SSM may consult with SMC/SES.

3.4. Systems Acquisition (EMD through P&D). The SSM must be familiar with the activities and documentation generated in Systems Acquisition. As required in every major program phase, 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/IMS) and the SSMP/SSPP. The SSM must participate in the following activities:

3.4.1. The SSM will review and update the government program documentation in order to re-align system safety objectives for currency and consistency. The SSM will review and update key program documents including the following: SSMP, PHL, SEP, PESHE, HSIP, TEMP and CARD.

3.4.2. In support of contracting for the systems acquisition phase, the SSM will develop criteria for proposal review/evaluation and participate in the source selection.

3.4.3. RFP Input For The Systems Acquisition Contract. In pre-contract activities, the SSM will ensure that system safety verbiage and data requirements needed at the systems acquisition phase are reflected in the RFP package to include the contents of the GSOW, CDRLs and Sections L and M.

3.4.4. The SSM will ensure that the tasks in this phase include updates of the SSPP, PHL and PHA and will add new CDRLs that include the Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA) and the Operating & Support Hazard Analysis (O&SHA). Other CDRLs that may be required at this point include the Explosive Hazard Classification (EHC) Data, Missile System Prelaunch Safety Package (MSPSP), Flight Data Package (FDP), Environmental Analysis Report, Preliminary Test Reports, Engineering Change Proposal System Safety Report, Waiver or Deviation System Safety Report, and specification updates reflecting complete system design. The SSM must check data submittal requirements necessary to be delivered at different geographical test and operational sites. Launch vehicle and satellite programs will require Range Safety data packages such as MSPSPs and FDPs. Other programs may require Accident Risk Assessment Reports

(ARAR) or Mishap Risk Assessment Reports (MRAR) or Safety Assessment Reports (SAR) in addition to the typical hazard analyses data.

3.4.4.1. The SSM will ensure that required system safety related assessments and data submittals supporting operations and end-of-life actions are included as contract data deliverables. These data include the Space Debris Assessment Report (SDAR) and End-of-Life Plan (EOLP). The SSM will also provide input to the contract to ensure the timely delivery of these data. For example, a CDR Draft SDAR is required 45 days before CDR.

3.4.5. The SSM will ensure that the Offeror's instruction in the RFP include how system safety will be addressed in program management and systems engineering program execution to include narratives addressing event-driven tasks and products through the IMP/IMS and CWBS. System safety representations from engineering and management review boards will be depicted.

3.4.6. The SSM must participate in the source selection process. If the SSM is not allowed to participate, the PM or PSM will assume the responsibility. System safety criteria for the source selection must reflect instructions addressed in the RFP.

3.4.7. Data submittal review/approval. The SSM will be involved in the review and approval of data submittals. The SSM will be included in the Systems Directorate coordination process concerning system safety data comments, disposition and approval.

3.4.8. In this phase, in order to implement a comprehensive system safety program, other Systems Acquisition activities will also be accomplished to complement pre-contract and contract related activities. These activities include the following:

3.4.8.1. Maintaining the SSG and SSWG during the EMD stage. The PM or PSM and the SSM will ensure that the charter for the System Safety Group (SSG) is updated and approved for implementation.

3.4.8.2. Continue validating the scope of the system safety program, including contractual requirements and deliverable system safety data.

3.4.8.3. Ensure all appropriate managers consider and document the long-term consequences of hazards.

3.4.8.4. Ensure that an overall safety assessment is provided before each milestone or program review.

3.4.8.5. Review and evaluate engineering change proposals and requests for deviation or waivers.

3.4.8.6. Identify and establish SSWGs as necessary, to work detailed system safety issues.

3.4.8.7. Assigning mishap or hazard-risk indices to each SSG discussion and action item.

3.4.9. In Systems Acquisition, the SSM will also participate in the technical and management reviews established by both the government and contractor. These reviews have attributes (cost, workbreakdown structure, schedules, system functions/specifications, risk resolutions, etc.) affecting system safety and they should include the following:

3.4.9.1. Integrated Baseline Review (IBR). A joint assessment conducted by the government PM or PSM and the contractor to establish the Performance Measurement Baseline (PMB).

3.4.9.2. Flight Readiness Review (FRR). SMC/SE provides coordination and consultation on Space Flight Worthiness Criteria (SFWC) documentation upon request and when personnel are available.

3.4.9.3. Test Readiness Review (TRR). The SSM will participate in the assessment of test objectives, test methods and procedures, scope of tests, and safety to confirm that required test resources have been properly identified and coordinated to support planned tests. The TRR is a multi-disciplined technical review designed to ensure that the subsystem or system under review is ready to proceed into formal test.

3.4.9.4. Critical Design Review (CDR). The SSM must participate in the CDR process to ensure that system safety interests have been considered in the establishment of product baselines to satisfy Capability Development Document requirements within allocated budget and schedule.

3.4.9.4.1. The SSM must ensure at the CDR that the process evaluates the proposed baseline ("Build To" documentation) to determine if system safety design have been integrated in the documentation (Initial Product Baseline, including Item Detail Specifications, Material Specifications, Process Specifications) in a satisfactory manner to start initial manufacturing.

3.4.9.4.2. At CDR or immediately prior to CDR, the SSM must ensure that all system safety technical risks will be reduced to acceptable levels and that the remaining program execution risk resulting from resource or schedule shortfalls will be addressed quickly. Use of formal Engineering Change Proposals (ECPs) will likely be needed to resolve system safety deficiencies after CDR; thus, requiring more coordination that may impact cost and schedule.

3.4.9.5. System Verification Review (SVR). The SSM will participate in the SVR to ensure that system safety risks are acceptable for the system to proceed into Low-Rate Initial Production and Full-Rate production. The SVR establishes and verifies final product performance and provides input to the Capability Production Document (CPD).

3.4.9.6. Functional Configuration Audit (FCA). The SSM should participate in the FCA, a formal examination of the “as tested” characteristics of the configuration items (hardware and software) with the objective of verifying that actual performance complies with identified and documented system safety design and interface requirements. A successful FCA typically demonstrates that the EMD product is sufficiently mature for entrance into Low-Rate Initial Production.

3.4.9.7. Production Readiness Review (PRR). The SSM should participate in the PRR to ensure that system safety design requirements have been adequately incorporated for production and if the prime contractor and major subcontractors have accomplished adequate system safety in production planning without incurring unacceptable risks.

3.4.9.8. The SSM will implement a system safety acquisition strategy using a SMC/SES developed template. For assistance, the PM or PSM or the SSM shall consult with SMC/SES.

3.4.9.9. Another major activity in Systems Acquisition involves the Production and Deployment (P&D) phase. In the P&D phase, the SSM should participate in the Operational Test Readiness Review (OTRR) to ensure that system safety risk issues have been resolved so the system can proceed into initial OT&E with high probability of success to prove that the system is effective and suitable for service introduction.

3.4.9.9.1. Also, another activity in the P&D phase that the SSM should participate in is the Physical Configuration Audit (PCA). Since the PCA examines the actual configuration of an item being produced, the SSM should verify that the related system safety design documentation matches the system safety items (system, subsystem, components, software, and hardware) as specified in the contract. The SSM should confirm that adequate and approved system safety design are inherent, adequately planned, tracked, and controlled in the manufacturing process, quality control system, measurement and test equipment/process, training and operations. The SSM will ensure that the inherent/designed-in system safety items will pass and withstand test and operational stresses. Additionally, fail-safe system attributes must work.

3.4.9.10. The SSM must also ensure that identified system safety risks are being processed and being elevated to the appropriate risk review boards and system engineering review boards.

3.5. Sustainment (O&S Phase). In the Operations and Support (O&S) phase, the SSM will perform continuous surveillance on the existing system safety program. The SSM will implement in-service management metrics to validate the robustness of the system safety program or to reveal system safety program deficiencies or weaknesses. Sustainment and disposal work efforts make up the Operations and Support phase which is the final phase and extends throughout the useful life of the system.

3.5.1. System Safety Metrics. The SSM will implement system safety metrics that reveal system safety program information and status ensuring that:

3.5.1.1. The defined system safety management process identifies and prioritizes all appropriate system safety issues.

3.5.1.2. The defined system safety management process identifies the appropriate technical resources to staff all appropriate issues and that the resources are available and adequate for mitigations.

3.5.1.3. The defined system safety management process supports the technical resources to accomplish system safety action item resolution.

3.5.2. In the O&S phase, the SSG (utilizing accumulated system safety data from operational experience) should assist the Systems Directorate in evaluating results of failure analyses and mishap investigations. The SSM should participate in deficiency review and resolution activities.

3.5.2.1. The SSM will update hazard analyses to reflect changes in risk assessments, and to identify any new hazards, based on actual experience with the system and ensure that safety implications of the changes are considered in all configuration control management actions.

3.5.2.2. The SSM will make recommendations to updates of system safety documentation, such as design handbooks, military standards and specifications, to reflect safety "lessons learned." The SSM should share the information at the SSG and SMC System Safety Manager's Council meetings.

3.5.2.3. The SSM should document hazardous conditions and system deficiencies for development of follow-on requirements for modifications and new systems.

3.5.2.4. The SSM will evaluate proposed and new operating and maintenance procedures, or changes, to ensure that procedures, warnings, and cautions are adequate and inherent safety is not degraded.

3.5.2.5. The SSM must ensure that safety reviews are conducted periodically or in response to the user's current safety problems to identify the scope and frequency of the problem and possible solutions.

3.5.3. Demilitarization and Disposal. When the system reaches the end of its useful life, the system will be demilitarized and disposed of in accordance with all legal and regulatory requirements and policy relating to safety of personnel, property, the public and the environment. System safety activities will shift to concerns of demilitarization, de-arming, and disposal risks.

3.5.3.1. SSG meetings will provide a focal point for bringing together diverse expertise to address demilitarization and disposal issues. In preparation, the SSM will review and update disposal plans and analyses generated at the early stages of the system life cycle to include development and production. Initial termination concepts must be updated with current applicable laws and policy.

3.5.3.1.1. The SSM will apply knowledge obtained from operations, maintenance, mishaps, high accident potentials (HAPs) and anomalies and recommended mitigations.

3.5.3.2. The following are some specific end-of-life system safety activities that the SSM should perform:

3.5.3.2.1. Establish the limits of damage or injury capability of a system or subsystem.

3.5.3.2.2. Identify the special procedures and equipment needed for handling and disposal. Prepare instructions for implementing the plan.

3.5.3.2.3. Determine whether or not the material or its construction can be safely reused.

3.5.3.2.4. Identify the characteristics and amounts of hazardous materials present in the system.

3.5.3.2.5. Determine the current service requirements for destruction.

3.5.3.2.6. Determine whether societal impacts will occur in civilian areas.

3.5.3.2.7. Determine the availability of disposal sites for hazardous materials.

3.5.3.2.8. Ensure that current local, state, and federal laws are applied to disposal and demilitarization efforts.

3.5.3.2.9. Determine the adequateness of the End-of-Life Plan (EOLP) IAW AFI 91-217 requirements.

Chapter 4

SYSTEM SAFETY KEY FUNCTIONS

4.1. System Safety Functions. Chapter 3 discussed the involvement of system safety throughout the life cycle of a system. This section outlines organization of system safety objectives into three functional groups applied throughout system life cycle. They are summarized in the table below:

Table 4.1. System Safety Functional Groups.

Management	Task areas: planning, control, risk management and information management. Primarily involved with organization, personnel, risk management, task planning, scheduling, authorization, communication and monitoring.
Engineering	Task areas: requirements, analysis and design. Primarily involved in policy interpretation for design guidance, hazard identification & analysis, and mishap risk mitigation/verification.
Operations and Testing	Task areas: testing, fielding, sustainment, operational use and maintenance. System safety tasks involved in operations and testing include the test safety review board process, space flight worthiness criteria, and deficiency reporting and corrective actions.

4.2. System Safety Management and Planning. System safety program management and plans will be documented in the SSMP and augmented by specific sections in the SEP, TEMP, HSIP, PESHE, CARD, WBS and the RFP. In most if not all cases, the SSM shall generate the required input to all these documents. The SSMP and the PESHE are the two main documents that provide a roadmap on how to conduct and validate the system safety program.

4.2.1. System Safety Management Plan (SSMP). The SSMP will contain the Systems Directorate's or Division's system safety management requirements and tasks. The SSMP will be prepared by the Systems Directorate's SSM and approved (signed) by the Systems Director after the coordination (signed) with the Director of Safety (SMC/SE). An approved copy will be provided to SMC/SE for evaluation and use for the Systems Directorate system safety program metrics. The initial release of the SSMP will authorize the initial set of government system safety tasks. (See Table A2.2 for a SSMP outline)

4.2.1.1. The SSM must be given the appropriate authority, resources and responsibility to implement the SSMP. Each SSMP will, as a minimum:

4.2.1.1.1. Identify contractor and government roles, responsibilities and personnel qualifications which can be broken down further as follows:

4.2.1.1.1.1. Organizational structure and responsibilities (reporting chain, decision making, resource allocations, etc.).

4.2.1.1.1.2. Personnel qualifications (see Table 4.2 of this SMCI).

4.2.1.1.1.3. Manpower authorizations by skill types, need dates and required training.

4.2.1.1.1.4. Resource loading including manning and funding for the life cycle.

4.2.1.1.1.5. Authority and accountability for implementing tasks and risk decisions.

4.2.1.1.2. Identify system safety critical design and operations that include:

4.2.1.1.2.1. Requirements and criteria for status assessment of controls/mitigations.

4.2.1.1.3. Identify safety milestones and key documentation consisting of:

4.2.1.1.3.1. Requirements for schedule control and reporting.

4.2.1.1.3.2. Requirements and criteria for beginning and ending milestones for defined safety critical system safety tasks.

4.2.1.1.3.3. Required management and technical reviews describing:

4.2.1.1.3.3.1. Roles of Integrated Product Teams (IPT) during reviews.

4.2.1.1.3.3.2. System safety integration in program management and systems engineering.

4.2.1.1.3.3.3. Entry and exit criteria. Entry criteria (1) defines the minimum system safety essential items necessary to enter into a design review, (2) defines the system safety design baseline and provide the system safety framework for the design review, and (3) covers system safety items specified in the Statement of Work, the Specification, and the requisite system safety CDRL items describing design. Exit criteria (1) defines the minimum system safety essential items necessary to successfully complete a design review and proceed into the next phase and also (2) include system safety items specified in the Statement of Work, the Specification, and the requisite system safety CDRL items describing the design.

4.2.1.1.4. Describe liability and indemnification strategy.

4.2.1.1.5. Describe the integration of both government and contractor(s) system safety processes to form a single system safety program including:

4.2.1.1.5.1. How the SSMP requirements flow down to the contractor system safety program.

4.2.1.1.5.2. Describing the relationships and interfaces with related efforts inherent in contractor system safety programs and plans.

4.2.1.1.6. Describe the identified contractual system safety and health requirements.

4.2.1.1.7. Describe the defined Contractor’s role and scope of involvement in mishap investigation.

4.2.2. Programmatic Environment, Safety and Occupational Health Evaluation (PESHE). The system safety sections of the PESHE will complement and validate the SSMP.

4.2.2.1. In the PESHE, the PM or PSM will validate that appropriate HSI and ESOH efforts are integrated across disciplines and into systems engineering to determine system design characteristics that can minimize the risks to the system and personnel and enhance system safety and job performance and productivity of personnel. The PM or PSM will also validate planning for the system's demilitarization and safe disposal.

4.2.2.2. The PESHE will validate, as a minimum, the existence and effectiveness of the following safety and health requirements:

4.2.2.2.1. A strategy for integrating Environment Safety and Occupational Health (ESOH), which includes system safety, Operations Safety and Health, Operational Safety, Suitability, and Effectiveness (OSS&E), and Explosive Safety.

4.2.2.2.2. The ESOH responsibilities for implementing this strategy.

4.2.2.2.3. A process to identify ESOH hazards to assess risks, to mitigate or avoid those risks, to accept the residual risk, and to assess the effectiveness of the mitigations.

4.2.2.2.4. A process to identify and status ESOH risks (including the identification of hazardous materials used in the system and the plan for their demilitarization/disposal).

4.2.3. The system safety program will also include the necessary planning, coordinating, and engineering analysis to:

4.2.3.1. Identify the safety-critical functions of the system and establish a protocol of analysis, design, test, and verification & validation for those functions.

4.2.3.2. 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.

4.2.3.3. Identify, document and track system and subsystem-level hazards.

4.2.3.4. Identify the system-level effects of each identified hazard.

4.2.3.5. Categorize each identified hazard in terms of severity and probability of occurrence (specify qualification or quantification of likelihood).

4.2.3.6. Conduct in-depth analysis to identify each failure pathway and associated causal factors.

4.2.3.6.1. Analysis will be conducted to the functional depth necessary to identify logical, practical and cost-effective mitigation techniques and requirements for each failure pathway initiator (causal factor).

4.2.3.6.2. Analysis will also consider all hardware, software, and human factor interfaces as potential contributors.

4.2.3.7. Derive safety-specific hazard mitigation requirements to eliminate or reduce the likelihood of each causal factor.

4.2.3.8. 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.

4.2.3.9. Conduct a safety assessment of all residual safety risk after all design, implementation, and test activities are complete.

4.2.3.10. Conduct a safety impact analysis on all Software Change Notices (SCN) or ECP for engineering baselines under configuration management.

4.2.3.11. 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.

4.2.3.12. Submit for approval to the acquiring authority an integrated system safety schedule that supports the program's engineering and programmatic milestones.

4.2.4. System Safety Management Structure, Elements and Functions. System Safety will be the responsibility of the Systems Director or Program Manager (PM) or Product Support Manager (PSM). The Government System Safety Manager (SSM) will manage the system safety effort on his/her behalf, and as such is considered a "direct report" to the Systems Director or PM or PSM while performing this function. In the absence of a SSM, responsibilities roll up to the Systems Director or PM or PSM.

4.2.4.1. The Systems Director or PM or PSM will appoint his/her SSM in writing, in an appointment letter addressed to SMC/SE, requiring the concurrence of the SMC Director of Safety. Adequate data will be attached to assure the qualifications of the SSM. A template of the appointment letter and qualifications will be provided upon request.

4.2.4.1.1. Qualification requirements for a SSM are listed in Table 4.2. SMC/SES can assist in the creation of any waiver packages for the SSM appointment.

4.2.4.1.2. SMC/SE concurrence may be withheld or withdrawn due to reasons such as unmet qualification requirements, failure to perform duties, or inappropriate performance of duties (e.g. falsification of documents), in which case a different person must be assigned.

4.2.4.1.3. A SSM serving part time, assisting the primary SSM or in a geographically separate location sometimes referred to as a System Safety Officer (SSO) must meet the same qualification requirements.

4.2.4.1.4. There must be at least one responsible full time SSM per Systems Directorate, Program Office, Systems Division, or equivalent.

4.2.4.2. The system safety management function will be responsible for identifying safety information and reporting/coordinating the information within the program office (systems engineering, quality, reliability, configuration management, procurement, etc.). The SSM will coordinate with SMC/SES and contractors' safety organizations. This function ensures planning and implementation efforts satisfy program requirements.

4.2.4.3. The PM or PSM will be responsible for ensuring that the System Safety function within his/her 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 (PEO).

4.2.4.4. The SSM's Roles and Responsibilities. The SSM will be responsible for day-to-day management of the System Safety Program on behalf of the Systems Director or PM or PSM.

4.2.4.4.1. The PM or PSM and the SSM will ensure that identified mishap risks are documented, appropriately categorized in accordance with established and approved mishap risk category criteria and reported to the defined authority levels for action. The defined authority levels are the Service Acquisition Executive (SAE) for High, the Program Executive Officer (PEO) for Serious and the Program Manager (PM) or Product Support Manager (PSM) for Medium Mishap Risk Categories. Mishap Risk Categories considered "Low" will be managed "as directed." Mishap Risk Categorization and authority levels for actions are further defined in Tables A2.7, A2.8, A2.9 and A2.10 of this SMCI.

4.2.4.4.2. The scope of the SSM's responsibility will include coordination of government (Systems Directorate/Division, 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, subcontractor, and vendor safety organizations and individuals throughout the lifetime of the system.

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

4.2.4.4.3.1. Necessary system safety manpower support (Government, Aerospace, SETA contractor).

4.2.4.4.3.2. Any required system safety training.

4.2.4.4.3.3. TDY attendance (Systems Directorate and invited guests) at any reviews, and meetings requiring system safety participation.

4.2.4.4.3.4. Planning estimates of the Prime Contractor's system safety costs.

4.2.4.4.4. The SSM will interface with other Systems Directorate's internal organizations on other aspects of program management, systems engineering, contracts, including configuration management, quality assurance, test & evaluation, and reliability & maintainability to ensure that system safety engineering and policy requirements are included in all applicable Systems Directorate activities.

4.2.4.4.5. The SSM will interface with other SMC organizations including SMC/SE, and other Systems Directorate SSMs or SSOs to identify common SMC system safety issues and to formulate system safety policy to resolve these issues.

4.2.4.4.6. The SSM will also interface 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.

4.2.4.4.7. The SSM will coordinate system safety activities such that contractor and government personnel will all typically participate in a single team effort for systems engineering, systems safety engineering and mishap risk control and acceptance.

4.2.4.4.7.1. Typical roles of prime contractors include performance of technical

analyses, and day-to-day participation in design and development efforts.

4.2.4.4.7.2. Typical roles of government, SETA and FFRDC personnel include requirements development and review and verification of a contractor's plans technical analyses and reports.

4.2.4.5. Systems Directorate personnel will be properly trained on the Systems Directorate's unique processes and tools. The Systems Director or PM or PSM will ensure that his/her personnel have access to processes and tools (e.g. Hazard Log Database) needed to perform the work.

4.2.4.6. SMC/SE assists system safety personnel in obtaining appropriate training.

4.2.4.7. Individuals assigned system safety responsibilities in the Systems Directorate (e.g. both government and contractor) must have the appropriate qualifications (See Table 4.2) to properly perform their system safety functions. The Systems Directorate's system safety staff will ensure that similar requirements are flowed down to the product/system contractor for implementation. The acquisition certification requirement may not apply for product/system contractor key System Safety personnel but is desirable.

4.2.4.8. Qualifications for key system safety personnel (including SSMs, SSOs and SSEs) must 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 4.2. Minimum Qualifications For 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: Application for Waivers will be processed by the SMC Chief of System Safety (SMC/SES). Applications must include justification (e.g, lack of personnel, oversight by qualified person) and required developmental path to qualification for the applicant. Contact SMC/SES for examples.

@ Most SMC programs are of high complexity and hazard potential. All programs will be classified "High" unless justification is approved by the SMC Chief of System Safety (SMC/SES).

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 Directorate, Systems Division, or equivalents) must include the USAF System Safety Analysis Course and System Safety Management course or 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, and other available certification equivalence approved by SMC/SES.

4.2.4.9. Contractual Functions. The SSM will work with contract and data management organizations to place MIL-STD-882 on contract and to apply the necessary tasks, CDRLs, and other requirements to define an appropriate and adequate Systems Directorate system safety program. This SMCI is intended to enable the user to apply the necessary standards or versions of standards to comply with multiple higher-level instructions, using the best available tools for the program while maintaining clear compliance with current methodologies. This may require using tasks and other tools of MIL-STD-882C along with language referencing the latest MIL-STD-882C. AFI 91-202_AFSPCSUP1_I instructs PMs or PSMs to implement and integrate a government System Safety Management Plan with their contractor's MIL-STD-882C-Tailored System Safety Program. DoDI 5000.02 also states that, "The PM or PSM shall use the methodology in MIL-STD-882D, "DoD Standard Practice for System Safety." MIL-STD-882C is linked with older versions of DIDs than the ones currently listed on DOD websites, while MIL-STD-882D is not associated with any DIDs. This SMCI applies the updated DIDs and adopts the requirements from both MIL-STDs-882C & D for tailoring the needed Systems Directorate system safety program. Provided manpower support is available, assistance can be requested from SMC/SES in establishing which MIL-STD-882 requirements and DIDs are suitable for application to a specific program. It should be noted that other System Safety standards such as the industry standard ANSI/GEIA 0010 now exist; SMC/SES personnel can advise on appropriate application of these standards.

4.2.4.9.1. MIL-STD-882C/D Tailoring and Associated CDRLs and DIDs. MIL-STD-882C/D will be tailored by the SSM specific for the system's system safety program. MIL-STD-882C/D describes the management of all contractor system safety programs for the Department of Defense. Generally, MIL-STD-882C/D requires the contractor to establish and implement a system safety management system with system safety objectives and approaches consistent with mission

requirements with desired results in a timely and cost effective manner. Desired data submittals are also obtained by the application of a data management process in which information is provided in certain configuration/format as depicted and delineated by applicable DIDs. MIL-STD-882C/D discusses the system safety tasks; however, the entire document is not used for every system safety program. Applying the entire document will generally not be prudent because some requirements may not be needed for the specific system. Some requirements may be too excessive and will just add unwanted costs. At other times requirements language that is additional or different from the standard may be best for a specific program. Therefore, the authors of the document strongly recommend to tailor for specific programs.

4.2.4.9.2. Tailoring MIL-STD-882C/D Tasks. The SSM will tailor the MIL-STD-882C/D Tasks to better accommodate the program being supported. Tailoring allows for a system safety process that is customized to the specific program, by which mission success, timely schedule and cost savings can be realized.

4.2.4.9.2.1. The Systems Director will be responsible in ensuring that funding is made available in order to perform those identified tasks. The sections of tasks described by MIL-STD-882C/D include program management and control, design and integration, design evaluation, and compliance verification.

4.2.4.9.2.2. The System Safety section of the Government Statement of Work included in the RFP is where the tailored MIL-STD-882C/D task list should be located.

4.2.4.9.3. The SSM will ensure that the Contractor will develop and implement a System Safety Program Plan (SSPP), per the MIL-STD-882C/D (Tailored), that clearly states how their System Safety Program will be conducted, to include hazard analysis for the system throughout its lifetime, addressing both hardware and software system safety.

4.2.4.10. Data Item Description (DID) and Contract Data Requirements List (CDRL). The SSM will select, tailor and apply the required DIDs in order to obtain the necessary data submittals. 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 linked directly to MIL-STD-882C tasks include but not limited to DI-SAFT-80100A (SSPP), DI-SAFT-80101A (System Safety Hazard Analysis Report), DI-SAFT-80102A (SAR), DI-SAFT-80103A (ECPSSR), DI-SAFT-80104A (Waiver/Deviation SSR), DI-SAFT-80105A (SSPPR), DI-SAFT-80106A (HHAR). DID DI-SAFT-80100A became DI-SAFT-81626 when a DID for SSPP was required for use with MIL-STD-882D. The DIDs with the “A” suffix were numbered with “B” suffix in the late 1990s when they were updated for use with later versions of MIL-STD-882. The “B” DIDs eliminated reference to the System Safety Program Plan DID; during this period a policy (since abandoned) existed that SSPPs and other plans could not be

obtained as part of a contract. (The user of "B" DIDs should take care not to inadvertently leave out reference to a desired SSPP due to the nature of these DIDs). DIDs describe the data content and format. The most common DIDs used in system safety are described below:

4.2.4.10.1. *DI-SAFT-80100A System Safety Program Plan (SSPP).* The "A" revision of this DID is linked with MIL-STD-882C and 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.

4.2.4.10.2. *DI-SAFT-81626 System Safety Program Plan (SSPP).* This DID was written to re-establish a DID requiring the SSPP, and is widely used for this purpose after the establishment of MIL-STD-882D. As in the previous paragraph, 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. The main difference between DI-SAFT-80100A and DI-SAFT-81626 is that DI-SAFT-81626 allows the use of contractor data submittal format. DI-SAFT-81626 language also makes reference to "craft" (e.g. Navy vessels) and is written in the context of modification to an existing system. Organizations tailoring this DID need to take care that the tailoring fits the format requirements and the nature and phase of the system and program it's being tailored for.

4.2.4.10.3. *DI-SAFT-81300/A 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 version without letter suffix is listed in MIL-STD-882C as associated with that standard. The data resulting from these tasks and compiled into the MRAR are applicable to the system design, test, processing and operations within a contract.

4.2.4.10.3.1. For programs involved with Range Safety approval process, a MSPSP may be the preferred data to be submitted to the Range(s) over the MRAR. The MRAR could then be formatted to have two parts; Part 1 will be the MSPSP and Part 2 will be the rest of the required contents for the MRAR. The MSPSP will then be submitted to the Range(s), but, both Part 1 and Part 2 will

still be required to be submitted to the Systems Directorate.

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

4.2.4.10.5. *DI-SAFT-80101B 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.

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

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

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

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

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

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

4.2.4.11. As a quick reference for programs applying MIL-STD-882C, the relationship between MIL-STD-882C Tasks and the DIDs that support them can be summarized in Table A2.17 (MIL-STD-882C Tasks and Data Item Descriptions Matrix) in Attachment 2.

4.2.4.12. A matrix showing how each of the DIDs supports the various MIL-STD-882C tasks is also located in Table A2.16.

4.2.4.13. Based on the level of system safety to be performed, there are basically two types of system safety programs defined at SMC. 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 Tables A2.12 and A2.13.

4.2.4.14. Compliance and Reference Documents. The SSM must ensure that the right compliance or reference document is cited for the appropriate requirement. For example, MIL-STD-882D is a management type system safety compliance document. It describes "how to" manage a system safety program. On the other hand, MIL-HdBk-454B defines the criteria a component, subsystem and/or a system should be designed to in order to achieve the required performance attribute that promotes safety or make the system fail-safe. Also, if Air Force personnel are involved in the construction, operation, maintenance and disposal activities, apply Air Force Occupational Safety and Health (AFOSH) Standards appropriate for the encountered hazards. For example, apply AFOSH 91-501 (Air Force Consolidated Occupational Safety Standard) for general industry type activity and apply AFOSH STD 48-9 (Radio Frequency Radiation Safety Program) when prevention of possible harmful effects of radio frequency (RF) exposure is required. Please note, SMC/EN maintains the latest list of Specifications and Standards for application to SMC Requests for Proposal and contracts in consultation with SMC/SE; consult the list for potential updates. In accordance with the SMC Specifications and Standards List, the following compliance and reference documents may be included as part of the Request for Proposal:

4.2.4.14.1. Compliance:

4.2.4.14.1.1. MIL-STD-882C, "System Safety Program Requirements (Tailored), 19 January 1993.

4.2.4.14.1.2. MIL-STD-882D, "Standard Practice For System Safety", (Tailored) 10 February 2000.

4.2.4.14.1.3. AFSPCMAN 91-710, "Range Safety User Requirements" (Tailored), 01 July 2004.

4.2.4.14.1.4. MIL-STD-1472F, "Human Engineering" (Tailored), 23 August 1999.

4.2.4.14.1.5. MIL-STD-1576, "Electroexplosive Subsystem Safety Requirements and Test Methods For Space Systems" (Tailored), 31 July 1984 (Notice of Validation, 04 September 1992).

4.2.4.14.1.6. MIL-STD-1522A, "Standard General Requirements For Safe Design and Operation of Pressurized Missile and Space Systems" (Tailored), 28 May 1984 (Notice of Validation, 04 September 1992).

4.2.4.14.2. References:

4.2.4.14.2.1. AFI 91-202_AFSPCSUP1_I, 01June 2005; (Certified current 30 Jul

2007) Chapter 9, System Safety, and Chapter 11, Space Safety.

4.2.4.14.2.2. AFI 91-204_AFSPCSUP_I, 02 January 2007.

4.2.4.14.2.3. AFI 91-217, Space Safety and Mishap Prevention Program, 18 February 2010.

4.2.4.14.2.4. AFMAN 91-222, Space Safety Investigations And Reports, 09 August 2005.

4.2.4.14.2.4.1. AFMAN 91-222_AFSPCSUP_I, Space Safety Investigations And Reports, 02 January 2007.

4.2.4.14.2.5. AFOSH STD 91-50, Communications Cable, Antenna and Communications-Electronic (C-E) Systems, 01 August 1998.

4.2.4.14.2.6. AFOSH STD 91-501, Air Force Consolidated Occupational Safety Standard, 07 July 2004.

4.2.4.14.2.7. MIL-HDBK-454B, General Guidelines For Electronic Equipment, 15 April 2007.

4.2.4.14.2.8. SMC/CV Policy Letter, Mishaps at Contractor Facilities.

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

4.2.4.16. Other RFP/Contractual Items. The SSM will provide input to the other RFP/Contractual and related items listed below:

4.2.4.16.1. Acquisition Strategy Document (ASD).

4.2.4.16.2. Government or Contractor Statement of Work Award Fee.

4.2.4.16.3. Federal Acquisition Regulations (FARs).

4.2.4.16.4. DOD Contractor's Safety Manual for Ammunition and Explosives.

4.2.4.16.5. Technical Requirements Document (TRD), System and Subsystem Specs, Interface Control Documents.

4.2.4.16.6. Sample or Reference Mission(s).

4.2.4.16.7. Tasks.

4.2.4.16.8. Task Tailoring.

4.2.4.16.9. Indemnification Strategy.

4.2.4.16.10. Acquisition Strategy and Template.

4.2.4.16.11. Line items.

4.2.4.17. Request for Proposal Instructions to Bidders (RFP Section L). To meet RFP requirements, the SSM will coordinate in the Systems Directorate the tailoring of the safety items including those listed below as applicable to Section L. The SSM could

choose an option to impose the submittal of a draft SSPP with the proposal. SMC/SES can assist in the drafting of particular bidder instructions. The tailoring should impose that the Contractor describes the following:

4.2.4.17.1. Their 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.

4.2.4.17.2. Their relevant lessons learned.

4.2.4.17.3. For Launch Vehicle (LV) programs, their plan to support the Systems Directorate's efforts to satisfy LV system and range safety requirements.

4.2.4.17.4. For payload programs (e.g., satellites, secondary payloads, experiments, demonstrations), their plan to support the Systems Directorate's efforts to satisfy payload system and range safety requirements.

4.2.4.17.5. For ground control, network and facility systems, their plan to support the Systems Directorate's efforts to satisfy system safety requirements and obtain approval/certification.

4.2.4.17.6. For all programs, their plan to facilitate government system safety insight of all relevant contractor system safety activities and their plan to meet system safety personnel qualifications as prescribed by the requirements of Table 4.2 of this instruction.

4.2.4.17.7. For all programs, their proposed approach to develop an integrated Test and Evaluation (T&E) strategy that will be evaluated. Proposed approach must include system safety in a comprehensive, thorough, integrated, and documented program T&E plan.

4.2.4.17.8. For all programs, their proposed approach to develop an integrated training program, which includes system safety.

4.2.4.18. RFP Evaluation Criteria and Standards (Section M). Typically, evaluation criteria and standards for system safety will be included under the program management and system engineering sections. The following list will be included in Section M for use in the evaluation of:

4.2.4.18.1. The contractor's detailed description of the System Safety Program. The defined approach and specific processes, methodologies, major tasks, resources, techniques, tools, and criteria used to develop and implement the system safety program will be evaluated against criteria within MIL-STD 882C/D.

4.2.4.18.2. The 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.

4.2.4.18.3. The contractor's proposal in integrating system safety requirements in the systems engineering process.

4.2.4.18.4. The contractor's proposed approach to developing a T&E strategy. Their approach must include system safety in a comprehensive, thorough, integrated, and documented program in the T&E plan.

4.2.4.18.5. The contractor's proposed approach to develop an integrated training program which includes system safety.

4.2.4.18.6. The contractor's description of how they plan to support the Systems Directorate's efforts to satisfy range safety requirements for payload or launch vehicles as defined by the Systems Directorate's mission.

4.2.4.18.7. The contractor's detailed planning (for ground control, network, and facility systems) to support the Systems Directorate's efforts to satisfy all required system safety requirements and obtain all required approvals/certifications.

4.2.4.18.8. The contractor's description of lessons learned.

4.2.4.18.9. The contractor's description (for all programs) of their plan to facilitate the government's system safety requirements and tasks involving all relevant contractor system safety activities throughout program life cycle including on-orbit and disposal.

4.2.4.19. Work Breakdown Structure (WBS). The Government PM or PSM and SSM must ensure in the RFP's bidder's instructions that the contractor provides for a specific system safety WBS element.

4.2.4.19.1. The contractor's work breakdown structure (CWBS) must identify safety elements (tasking and level of effort) and will be consistent with system engineering requirements and schedules; the government PM/SSM will ensure this.

4.2.4.19.2. The SSM must be familiar with the detailed descriptions of both the Government's and contractor's WBS, and will 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.

4.2.4.20. Integrated Master Plan /Integrated Master Schedule. Both Government and Contractor System Safety tasks will be integrated into the program Integrated Master Plan and into the Integrated Master Schedule (IMP and IMS). Contractor's work packages will be consistent with the Government's system safety tasks.

4.2.4.20.1. The System Safety task scheduling must guarantee timely safety risk identification and control information to support valid management decision making. The task schedule will include: task title, phase (for example, Pre-A, A, B, C), milestone definitions, and inter task dependencies.

4.2.4.20.2. Each contractor system safety task will be authorized by inclusion in the government approved, contractor created System Safety Program Plan (SSPP).

4.2.4.20.3. Follow-on contractor tasks authorized by contract change(s) must be documented by changes to the approved SSPP. 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.

4.2.5. Risk Ranking, Tracking, and Residual Risk Acceptance. The Systems Directorate will develop and implement an integrated hazard/risk tracking process.

4.2.5.1. The results of this process will 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.

4.2.5.2. The identified hazards and mitigations will be tracked and managed throughout the entire program and system life.

4.2.5.3. The Systems Directorate will manage system safety hazard/risk identification and mitigation.

4.2.5.3.1. Appropriate risk acceptance authorities must be identified and decisions must be made and documented prior to the impacted mission or irrevocable action (e.g., launch or flight termination).

4.2.5.4. Risk handling, abatement, control, and/or resolutions strategies will be implemented to identify, evaluate, manage and/or resolve each risk, consistent with performance, cost and schedule.

4.2.5.5. Acceptance of residual risk shall be accomplished by signature of the appropriate managerial authority on a hazard report, as shown in Table A2.6.

4.2.6. Reviews and Meetings. The SSM and staff from SMC/SE shall be allowed access to, and may 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 Systems Directorate that may be germane to system safety, as determined by SMC/SE.

4.2.6.1. The SSM shall be included as a member of Program Engineering Change Proposal review and Configuration Control Boards (CCB).

4.2.7. System Safety Group (SSG). A SSG must be established (IAW AFI 91-202_AFSPCSUP1_I, Chapter 9) for all SMC acquisition programs that are ACAT 1 or equivalent. An SSG should be established for all projects (existing and future SMC space systems) that involve design, development, modification, evaluation, demonstration, testing, operation and disposal. It applies to all SMC missile, launch vehicle, satellites and ground facilities unless waived by AFSPC/SES through SMC/SE.

4.2.7.1. The SSG will be the method used by senior leadership to provide guidance and oversight to the Systems Directorate's system safety program.

4.2.7.2. The Systems Director, PM or PSM or the Deputy PM or PSM will chair the SSG. The SSG will be responsible for the following:

4.2.7.2.1. Evaluating the program System Safety status including funding.

4.2.7.2.2. Ensuring all appropriate managers consider and document the residual risks of hazards.

4.2.7.2.3. 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.

4.2.7.2.4. Reviewing the status of planned, pending, active, and disapproved safety modifications.

4.2.7.2.5. Reviewing and possibly approving or disapproving selected hazard analysis and their recommended controls and verification.

4.2.7.2.6. Reviewing high accident potential reports that have occurred since the last meeting.

4.2.7.2.7. Reviewing User/operator issues.

4.2.7.2.8. Reviewing the action item summary including action agencies and suspense dates; old and new action items.

4.2.7.2.9. Developing, coordinating 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 SSG and SSG membership)

4.2.7.2.9.1. The SSG will consist of the Systems Director/PM/PSM, the SMC Chief of System Safety, the Program SSM, and representatives from the using organization [i.e., HQ AFSPC, Numbered Air Force (NAFs), Centers, 30th and 45th Space Wings], Air Force Operational Test and Evaluation Center (AFOTEC), HQ AFSC and other DoD operators and users, including developers and users from industry organizations (see AFI 91-202 AFSPCSUP1).

4.2.7.2.10. Identifying and establishing SSWGs as necessary to work detailed safety risks.

4.2.7.3. The SSG will meet as required (at least annually) at the request of the government program manager or product support manager. Any member of the SSG may request that the program manager or product support manager call a meeting.

4.2.7.4. The SSG activities will be embedded in the Systems Directorate/Division SSMP.

4.2.7.5. The SSG/SSWG will include participation from all Systems Directorate stakeholders' organizations. Physical attendance at any SSG by SMC/SE personnel will be funded by the Systems Directorate.

4.2.7.6. The Systems Director or PM or PSM will be responsible for preparing minutes of SSG meetings and distributing them to SSG members and attendees within 30 calendar days of the meeting.

4.2.7.6.1. SSG minutes will be sent to the SMC Directorate of Safety (SMC/SE).

4.2.7.6.2. If a SSG meeting is not held on a major program within a year of the previous meeting, an explanatory letter must be sent to HQ AFSC (copy to AFSPC/SES and SMC/SES).

4.2.7.7. The System Safety Working Group (SSWG). IAW AFI 91-202_AFSPCSUP1_I, the government SSWG will be established by the SSG to work detailed safety issues.

4.2.7.7.1. The SSWG will be chaired by the SSM and does not generally require the attendance of the Systems Director or PM or PSM.

4.2.7.7.2. Typical SSWG activities will include: assessing the status of safety activities in the total system, various system segments, elements, subsystems and components. Hazards and their mitigations will be reviewed and disposed as follows:

4.2.7.7.2.1. Ill-defined hazards will be returned to the originator for clarification.

4.2.7.7.2.2. Valid hazards for which mitigation proposals have not been made will be assigned to an action officer, for mitigation.

4.2.7.7.2.3. Valid hazards that have been completely mitigated will be recorded; a hazard report form will be generated and presented to the appropriate risk acceptance authority for signature, and tracked until final disposition is reached.

4.2.7.7.2.4. Valid hazards that have been partially mitigated will be documented, assigned to an action officer and tracked until final disposition is reached.

4.2.7.7.2.5. Non-valid hazards and low hazard risks will be documented and archived.

4.2.7.7.3. Typical SSWG members will be government and contractor SSMs, 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.

4.2.7.7.4. The SSM will ensure that minutes of meetings are prepared and distributed to members and attendees within 30 calendar days after the date of the meeting.

4.2.7.7.4.1. System safety reviews, SSG/SSWG meeting minutes, and audit/inspection results will be written, distributed and stored in the Systems Directorate's system safety filing system or library.

4.2.8. System Safety Information Architecture and Maintenance. Systems Directorate activities will include a process for collecting, reviewing, auditing, analyzing, and sharing of system safety information and lessons learned. Required components will include, but are not limited, to:

4.2.8.1. System Safety Management Plan (SSMP) /System Safety Program Plan SSPP.

4.2.8.2. Preliminary Hazard List.

4.2.8.3. Preliminary Hazard Analysis Report (system safety, explosive safety and bioenvironmental).

4.2.8.4. Safety Requirements /Criteria Analysis Report.

4.2.8.5. Subsystem Hazard Analysis Report.

4.2.8.6. System Hazard Analysis Report.

4.2.8.7. Operating and Support Hazard Analysis Report.

4.2.8.8. Health Hazard Assessment Report.

4.2.8.9. Safety Assessment Report.

4.2.8.10. Test and Evaluation Safety Report.

4.2.8.11. Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation /Waiver.

4.2.8.12. Safety Compliance Assessment Report.

4.2.8.13. Explosive Hazard Classification and Characteristics Data.

4.2.8.14. Hazardous Material Management Program Report (HMMPR).

4.2.8.15. Hazard/Mishap Risk Assessment Matrix (H/MRAM).

4.2.8.16. System Safety Status Report.

4.2.8.17. Mishap Risk Assessment Reports (MRARs).

4.2.8.18. Missile System Pre-launch Safety Packages (MSPSPs).

4.2.8.19. Environmental Impact Statement or Environmental Impact Report.

4.2.8.20. Hazard Tracking Logs.

4.2.8.21. Space Debris Assessment Report (SDAR).

4.2.9. Hazard Tracking System. In the Systems Directorate, a hazard and mitigation tracking system will 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.

4.2.9.1. The Systems Director, PM or PSM and SSM will ensure that follow-up/close-out actions are appropriately tracked and documented.

4.2.9.2. The Systems Director, PM or PSM and SSM must ensure that management decisions for acceptance of residual risks are documented.

4.2.9.3. The hazard tracking system will provide “closed-loop” feed-forward/feedback control of hazards to assure that, for example:

4.2.9.3.1. Safety recommendations are actually implemented as hazard controls.

4.2.9.3.2. Test information is used to confirm or update system safety analysis.

4.2.9.3.3. Safety risks and safety control system performance levels, as determined by system safety analyses, will be validated or upgraded with ongoing mishap and system performance information.

4.2.9.4. Part of this tracking will 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 will be used later in the tracking process to assure that controls identified for each hazard are actually implemented.

4.2.9.5. The Hazard Tracking Log will summarize 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 Mishap Risk Assessment Values).

4.2.9.6. The Hazard Tracking Log will be used to track both design related and operationally related hazards.

4.2.9.6.1. 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) must be summarized as open hazards in the hazard log.

4.2.9.6.2. Hazards will be tracked from their identification (in the various hazards analyses, tests or operational experiences) throughout the system life cycle.

4.2.9.6.3. Hazard log entries will be continuously available for reference, and open entries will be presented at key milestones including program reviews.

4.2.9.6.4. All identified hazards must be verified closed prior to the phase of the mission when hazard exposure could occur or irrevocable action and decision will take place (e.g., launch).

4.2.9.6.5. Closure of each hazard will be denoted by the signature of appropriate contractor and government management on the associated hazard report.

4.2.9.6.5.1. 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:

4.2.9.6.5.1.1. The hazard has been eliminated through design, and the design action is verified, or,

4.2.9.6.5.1.2. 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,

4.2.9.6.5.1.3. The hazard has been assessed and noted. The risk has been accepted by contractor and government program offices and other stakeholders through the SSG.

4.2.9.6.5.1.4. Safety concerns affecting schedule, cost, system safety precedence, or requiring deviation or waiver to safety requirements have been appropriately resolved.

4.2.9.6.6. While historically paper forms have been used to track hazards, Systems Directorates and other organizations conducting acquisition functions are authorized and encouraged to operate and maintain hazard risk tracking database software. Each system must have a current log of identified hazards and residual mishap risk, including an assessment of the residual mishap risk. The tracking system for hazards, their closures and residual mishap risk must be maintained throughout the system life cycle. As changes are integrated into the system, the hazard log is updated to incorporate added or changed hazards and the associated residual mishap risk.

4.2.9.6.6.1. The Government must formally acknowledge acceptance of system hazards and residual mishap risk.

4.2.9.6.6.2. The SSM should reference MIL-STD-882C/D for contents of the hazard tracking system. Assistance can be provided by SMC/SES upon request if required support personnel are available.

4.2.9.7. It will be the responsibility of the Systems Directorate to maintain and use a log of all identified hazards and residual mishap risk, as part of their overall system safety program. This function must not be delegated to system development contractors, must be under the direct cognizance of the Systems Directorate and will be delineated in the SSMP. Maintenance and use of hazard logs by Systems Engineering & Integration (SE&I) and System Engineering Technical Assistance (SETA) contractors assigned to the Systems Directorate must have government oversight for the process to be considered "under the direct cognizance of the Systems Directorate."

4.3. System Safety Engineering. The system safety engineering function (as performed by a SSM, SSE, or other key safety personnel) must possess and maintain specialized knowledge and skills and apply engineering principles and techniques to identify, and eliminate or control system hazards and hazardous conditions, and verify the hazard mitigation in the following manner:

4.3.1. Integrating System Safety Engineering in Systems Engineering. System safety will be involved in systems engineering throughout the lifecycle, and system safety must be embedded as early as possible in the design.

4.3.2. The System Safety Manager (SSM) or System Safety Engineer (SSE) will perform analyses and makes technical recommendations throughout the life cycle, i.e., from concept design, development, build, operations, sustainment, and disposal.

4.3.2.1. Technical documents will be reviewed, evaluated, and corrected by the SSE to ensure design safety has been implemented.

4.3.2.2. System safety approval will 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.

4.3.2.3. The SSM or SSE interfaces with personnel from other specialties and will participate in milestone reviews that include SDR, PDR, CDR, TSR, MRR, FRR and LRR.

4.3.2.4. The SSM or SSE will also work with operational safety organizations and gather lessons learned throughout operations and disposal. Safety engineering data will be obtained from:

4.3.2.4.1. Existing analyses from other fields (such as FMECA from reliability).

4.3.2.4.2. Requirements (Air Force Instructions, MIL-STD's, etc.).

4.3.2.4.3. Mishap, high accident potential (HAP) and incident/anomaly data.

4.3.2.4.4. Lessons learned from similar or previous programs.

4.3.2.4.5. Test and development data.

4.3.2.4.6. System safety analysis.

4.3.2.4.7. Other sources (for example, reports on inspections/assessments, foreign object damage, deficiency, injury, maintenance and hazard & maintenance logs).

4.3.3. System Safety Design Criteria. The SSE will establish system safety design criteria. Recommendations for new system safety design criteria will be made using studies, analyses and test data.

4.3.3.1. System Safety design criteria will be used to further evaluate requirements if they are adequate, inadequate, or overly restrictive.

4.3.3.2. System Safety will use the Engineering Change Process to incorporate appropriate system safety related changes.

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

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

4.3.6. Software Safety. Software safety engineering activities will fully support and shall be fully integrated to 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.

4.3.7. Requirements Review, Allocation, and Traceability. Upon request, SMC/SES assists the Systems Directorate in developing a list of safety requirements documents for use by the SMC program office. The Program's uniquely tailored documents will be periodically updated as baselines, configurations, performance, and processes change. The following list identifies some of the Contractor-generated safety requirements documents.

4.3.7.1. The System Safety Program Plan, which demonstrates how the Contractor supports the Government system safety program.

4.3.7.2. The Hazardous Material Management Plan, which demonstrates how the Contractor supports the government hazardous material management program portion of the SSMP.

4.3.7.3. Hazard Reports and Hazard Analysis Reports, which define the safety risks found in the Program, and their associated controls.

4.3.8. Safety-related requirements can also be found in the Technical Requirements Document (TRD) and system and sub-system specifications.

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

4.3.9.1. AFI 91-202_AFSPCSUP1_I, The US Air Force Mishap Prevention Program.

4.3.9.2. AFI 91-204, Safety Investigations and Reports.

4.3.9.3. MIL-STD-882C/D, System Safety Program Requirements /Standard Practice For System Safety.

4.3.9.4. MIL-STD-1522A, Standard General Requirements For Safe Design And Operation Of Pressurized Missile And Space Systems.

4.3.9.5. MIL-STD-1540D, Product Verification Requirements For Launch, Upper Stage, And Space Vehicles.

4.3.9.6. MIL-STD-1576, Electroexplosive Subsystem Safety Requirements and Test Methods For Space Systems.

4.3.9.7. MIL-STD-1472F, Human Engineering.

4.3.9.8. MIL-HDBK 454B, General Guidelines For Electronic Equipment.

4.3.9.9. AFI 91-217, Space Safety And Mishap Prevention Program.

4.3.9.10. AFMAN 91-201, Explosives Safety Standards.

4.3.9.11. AFSPCMAN 91-710, Range Safety User Requirements.

4.3.9.12. DODI 5000.02, Operation of the Defense Acquisition System.

4.3.9.13. AFI 63-101, Acquisition and Sustainment Life Cycle Management.

4.3.9.14. AFI 63-1201, Life Cycle Systems Engineering.

4.3.10. The SSM must play an active role and be heavily involved in the requirements process. SSEs may be assigned to support the SSM to perform specific system safety engineering tasks. In the absence of SSEs, responsibilities roll up to the SSM. Activities will include:

4.3.10.1. *Review* - The SSM will review appropriate Program documentation to ensure system safety requirements have been properly incorporated.

4.3.10.2. *Allocation* - The SSE will ensure that tasks are allocated from safety requirements to the system specifications, the Contractor Statement of Work (CSOW) and other documents. The SSM 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.

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

4.3.11. Change Control. The SSE will be 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.

4.3.11.1. System safety impacts of proposed design changes will be considered in all government/contractor configuration control board actions.

4.3.11.2. A system safety assessment of design changes with recommended mitigations will be provided to the PM or PSM and the systems engineer.

4.3.11.3. Government SSE will be authorized to participate in government configuration control board meetings.

4.3.12. Mishap Risk Mitigation and Control. The SSE will ensure that the system safety order of precedence is applied in the mishap risk mitigation and control process. The system safety order of precedence, in descending order of preferred technique, includes:

4.3.12.1. *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 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.]

4.3.12.2. *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.

4.3.12.2.1. In the fault tolerance method, the design 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; an item (system, subsystem, component, or subcomponent) is designed in such a way that item failure or malfunction 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; the item (system, subsystem, component, or subcomponent) is designed such that prior to the item failing or malfunctioning at least three independent failures, or three human errors, or a combination of three independent failures and human errors must happen.

4.3.12.3. *Incorporate Safety Devices:* If the mishap risk can't be designed out, and engineering safety features don't work, the designer mitigates 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.

4.3.12.4. *Provide Warning Devices:* When design changes, engineered safety features, nor safety devices cannot 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.

4.3.12.5. *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 Systems Directorate, 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 Systems Directorate. Tasks and activities judged to be safety critical by the Systems Directorate 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.

4.3.13. Mishap Risk Verification. To ensure the mishap risk mitigations are acceptable for safety critical hardware, software, and procedures, the designer shall verify the mishap risk mitigations. The verification methods shall include test, analysis, inspection, simulation, and demonstration. 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. For clarification, the following verification processes are provided for guidance:

4.3.13.1. Test. System and subsystem testing shall be 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.

4.3.13.2. Analysis. 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. Analysis is a mathematical model of the system/subsystem/component operation with the risk mitigation incorporated. Analysis can be relatively inexpensive to conduct. Analysis can be used alone or in conjunction with each of the other verification methods. 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.

4.3.13.3. 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.

4.3.13.4. 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.

4.3.13.5. Demonstration. Demonstration is a very realistic mishap risk verification process as it is conducted to demonstrate that the inherent safety features of the system, subsystem or component work. Resources (processes, equipment, personnel, time factors, etc.) required to prepare for the demonstration should be equivalent to what is required in actual operation. Like the other verification processes, demonstration has limitations. For example, if demonstration is the only verification process applied, then, it would be similar to a fix-fly-fix process. The processes of verification should be

applied with "an order of precedence," (For example, perform the analysis first). For effect, a combination of the verification processes should be applied.

4.4. System Safety in Operations and Testing. Program management will ensure that the system can be safely tested and operated. Appropriate safety personnel will 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 acceptable safe levels.

4.4.1. Safety analysis and verification will be performed on facilities, equipment, requirements, specifications, documentation, procedural steps, necessary training and criteria to ensure and verify that the hazards are controlled. During operation or test execution, ensure safe performance of the operation or test.

4.4.1.1. The system safety management will implement 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.

4.4.2. Hazardous systems and subsystems that are to be tested must 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.

4.4.2.1. Test plans and objectives will 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.

4.4.3. Test Safety Review Board (TSRB) Process. The AFSPC/SMC TSRB will be conducted IAW AFI 99-103 and applied in conjunction with AFI 63-101, AFI 63-1201, AFI 91-217, AFI 91-202_AFSPCSUP1_I, AFMAN 63-119 and their supporting MAJCOM supplements and as applicable AFSPCMAN 91-710. The TSRB will provide an independent review of critical tests. 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.

4.4.3.1. The TSRB will determine which tests are safety-critical but in the case of a dispute SMC/SE will be the final SMC authority for determining which tests are safety-critical. If SMC/SE is not a member, the TSRB may consult with SMC/SE in determining which tests are safety-critical. The Systems Directorate TEMP and other test plans will identify safety-critical tests based on the unique risks created by, or mitigated using, that test. The Systems Directorate 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.

4.4.3.2. 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 will 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.

4.4.3.3. TSRB membership will include technically qualified system safety personnel who are organizationally independent from the test team or the organization executing the test activity. SMC/SE should be consulted as the SMC authority for determining who is technically qualified for system safety membership. Test plans for safety critical tests must not be released without TSRB approval.

4.4.3.4. The PM or PSM, in concert with the user and the T&E community, will provide safety releases to include a formal system safety risk acceptance to the developmental and operational testers prior to any test involving personnel. All system-related system safety risks must have been accepted at the appropriate management level prior to exposing people, equipment, or the environment to known hazards. A safety release must be provided to the Operational Test Agency (OTA) before start of dedicated operational testing. The safety release must transmit system safety hazard data to the operators, maintainers, and testers.

4.4.3.5. The PM or PSM must ensure that the system must be capable of being operated and maintained in its intended operational environment during dedicated operational testing with an acceptable level of system safety risks.

4.4.3.6. The PM or PSM must ensure that all system safety hazards with an assessed mishap risk level of "Serious" or "High" must be mitigated to an acceptable level and a safety release provided to the OTA before start of dedicated operational testing.

4.4.3.7. The PM or PSM must ensure that "The Logistics Support Concept (LSC)" and other Air Force concepts (Ref. AFMAN 63-119) must be reviewed and system safety constraints and limitations resolved.

4.4.4. Operational and Space System Safety. Systems Directorates will 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.

4.4.4.1. Systems Directorate System Safety personnel will 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. SMC Systems Directorates may have initial operational as well as developmental responsibilities. Since SMC's systems are almost always space systems or space-related systems, special safety requirements that apply to space systems will be observed.

4.4.4.2. Space Flight Worthiness Criteria (SFWC). Systems Directorate system safety and engineering personnel will participate in the development of SFWC, thresholds and targets for operational safety for their particular systems. SMC/SE representatives will assist if requested and provided that required resources are available.

4.4.4.3. Operational and Space Safety Tasks. Operational and Space System Safety personnel will 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 the Systems Director or PM or PSM and higher office processes.

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

4.4.5. Qualified People. Operational and space system safety personnel must meet qualification requirements that typically include training, experience, certification, education and/or other requirements. Training requirements that may apply include weapons safety training, space safety or orbital safety training. SMC/SE representatives can assist in verifying qualification requirements and obtaining training.

4.4.6. Establishing authority. Operational and space system safety personnel will assist management in establishing and maintaining authority for task accomplishment. Examples of authorizing documents that require safety input include SMC Instructions, Systems Directorate operating instructions, and program management guides or plans such as the SSMP.

4.4.7. Resources. Operational and space system safety personnel will assist management in obtaining resources, both manning and funding, to accomplish operational safety tasks. Manpower loading will 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 will be planned, budgeted and obtained as required.

Chapter 5

OTHER ACTIVITIES REQUIRING MAJOR SYSTEM SAFETY INVOLVEMENT

5.1. Other Activities and the System Safety Function. Paragraph 1.1.6. discussed the system safety relationship to other activities that included interfacing with external agencies such as the DoD Explosives Safety Board and the USAF Non-Nuclear Munitions Safety Board. At SMC, there are USAF mandated activities implemented at the SMC level. These activities require major system safety participation and include some of the following:

5.2. Orbital Operations and Safety. Orbital safety, in accordance with AFI 91-202_AFSPCSUP1_I, 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 as part of mission planning and in the design phase.

5.2.1. Orbital safety will also be implemented in accordance with AFI 91-217 (Space Safety and Mishap Prevention Program) and must cover on-orbit risks and mitigation plans including the following subject areas:

5.2.1.1. 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).

5.2.1.2. Directed Energy (minimize hazards or interference with spacecraft or the general public and property on the earth's surface or in the atmosphere).

5.2.1.3. Orbital Debris Minimization (minimize the generation of orbital debris during and after their service life).

5.2.1.3.1. 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).

5.2.1.4. 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.).

5.2.1.5. Human Factors (consider human factors in the design of the system and operations).

5.2.2. The Systems Directorate/Division will ensure that a Space Debris Assessment Report (SDAR) is generated prior to PDR and updated by CDR addressing timely resolutions of identified on-orbit hazard issues in order to minimize program cost and schedule impacts.

5.2.2.1. The SDAR and EOLP will address and meet requirements and criteria imposed by AFI 91-217.

5.2.2.2. The Systems Directorate will ensure that the SDAR and EOLP requirements are adequately addressed in the RFP and in data submittals.

5.2.3. To support the orbital safety effort and other aspects of mishap prevention in the orbital phase, an on-orbit phase hazard analysis describing possible hazards to, from, by or through the space system including the on-orbit asset (e.g. spacecraft) during on-orbit operations shall be generated by the contractor prior to PDR and updated by CDR.

5.2.3.1. 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 or Product Support Manager, for either resolution or acceptance by the Program Executive Officer. Program Risk notification must be submitted immediately after the discovery of the deficiency.

5.3. Programmatic Environment, Safety and Occupational Health Evaluation (PESHE). The SSM will ensure that the PESHE requirements from the different levels of instructions and standards (DoDI, AFIs, AFMANs) have been appropriately flowed down to the program/systems acquisition plans and specifications. The PESHE document is a requirement applicable to MDAPs and MAIS acquisition programs in accordance with DoDI 5000.02, Operation of the Defense Acquisition System. It is required to support major milestone decisions to include MS-B, MS-C, Full-Rate Production or Full Deployment activities. The PESHE enables DOD program offices to meet several statutory requirements including the National Environmental Policy Act (NEPA).

5.3.1. The SSM will apply the PESHE process in the program and should consult SMC/SE for interpretation of the system safety and health functions (and should consult SMC/EN for environmental functions) and activities to appropriately implement the evaluation process.

5.3.2. A separate SMC PESHE instruction (currently being written) will address the overall PESHE process.

5.4. Operational Safety, Suitability, and Effectiveness (OSS&E). Air Force Policy Directive 63-1, Acquisition And Sustainment Life Cycle Management, establishes the requirement for the Systems Director or Program Manager (PM) or Product Support Manager (PSM) to assure OSS&E of all systems and end items currently in or entering the operational inventory. Additionally, AFPD 63-1 mandates that the, "Air Force shall apply Systems Engineering processes and practices to all analysis and technical planning activities throughout the life cycle, from the development of concepts to meet user needs to system disposal." As such, it is the responsibility of the System Safety Manager to:

5.4.1. 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 OSS&E processes are found to have contributed to the mishap.

5.4.2. Ensure that appropriate System Safety policies and procedures are available for use in the acquisition process and for all systems and end-items.

5.4.3. Ensure that mishap investigation information and recommendations are provided to the responsible Program Manager or Product Support Manager for a system or end-item involved in a mishap.

5.4.4. Identify and communicate system and end-item safety hazards, risks, and recommendations to Program Managers or Product Support Managers and using commands/organizations for their assessment and action.

5.5. SMC Independent Readiness Review Team (IRRT). The SMC IRRT will provide for participation of SMC/SE representatives, and the Systems Directorate will provide resources as required for SMC/SE representative participation.

5.5.1. SMC/SE may participate on the SMC IRRT to provide independent System Safety Assessments of program activities, to ensure mishap prevention readiness and to share lessons learned.

5.5.2. SMC/SE will receive and be provided 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.

5.6. 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.

5.6.1. SMC Program Offices will obtain coordination or concurrence of safety documentation, to include any tailoring of such documents, with the applicable Range. SMC program offices should consult with SMC/SE for assistance as required.

5.6.2. Although these requirements are intended for Range Users and Operators, the SSM must ensure that any items brought to the ranges by the SMC Systems Directorate to support launch operations also comply with Range Safety requirements.

5.6.3. 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 Systems Directorate to ensure that funding is made available in order to perform both the tailoring activity and the proper execution of those tailored tasks.

5.6.4. Tailoring of AFSPCMAN 91-710 (or EWR 127-1 for legacy programs) will be conducted by the Contractor and/or the SSM, with concurrence from the applicable Range. Similarly, the tailoring for AFSPCMAN 91-711 will be conducted by the SSM. The Systems Directorate SSM may consult with SMC/SE for assistance as needed. The Ranges reserve final approval authority for tailoring these documents.

5.6.5. 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:

5.6.5.1. Incidents, near-misses, and mishaps (to include Investigation and Root Causes), particularly those involving pre-launch, launch, and post-launch operations.

5.6.5.2. Flight Termination Systems.

5.6.5.3. Launch Vehicle and Upper-stage debris or disposal.

5.6.5.4. Controlled re-entry of launch vehicles and upper stages.

5.6.5.5. Explosives, Propellants, and Pressure Vessels.

5.6.5.6. On-orbit safety analysis.

5.6.6. As part of the overall Program Office's 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.

5.7. 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.

5.7.1. There are several areas that a SSM should focus on with risk management. The SSM should perform the following for risk management:

5.7.1.1. Read, understand and be able to properly interpret and apply AFI 90-901_AFSPCSUP1_I (Operational Risk Management), 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.

5.7.1.2. 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.

5.7.1.3. Ensure that system safety issues, when identified and appropriate, are included in the Program Office's RM database.

5.7.1.4. Attend the scheduled risk management meetings and provide input to mitigation actions and risk rankings.

5.7.2. SSMs will provide guidance to the risk management team if and when necessary.

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

5.8. Interface with Air Force Operational Test & Evaluation Center (AFOTEC). For SMC programs that have AFOTEC involvement, close coordination between the Systems Directorate SSM, SMC/SE and AFOTEC/SE is key to a successful and safe operational test.

5.8.1. AFOTEC is a mandatory member of SSGs (IAW AFI 91-202). AFOTEC may require a copy of any safety documentation on the program in sufficient time prior to observing, participating or conducting tests. Typical safety documents required by AFOTEC/SE include, but are not limited to: safety certifications and reviews, PESHE, SSMP, SSPP, PHL, PHA, SSHA, SHA, O&SHA, SRCA, MRAR, MSPSP and the SAR.

5.9. USAF Deficiency Reporting, Investigation, and Resolution (DRI&R), T.O. 00-35D-54. The Systems Director or PM or PSM is responsible for implementing DRI&R IAW T.O. 00-35D-54. PMs or PSMs will ensure active oversight and awareness of DRI&R status and, depending on the category of the Deficiency Reports (DRs), the PM or PSM will either accept

the risk or recommend the acceptance of risk to the appropriate level of the chain of command prior to closing a DR. The PM or PSM will ensure members, of their assigned units, receive role-based DRI&R training as defined in T.O. 00-35D-54. PMs or PSMs are responsible for maintaining visibility of DRs reported against their system regardless of where the DR is assigned for resolution. The SSM will be an integral member of the DRI&R process for their system.

5.9.1. The SSM will coordinate and participate with the screening point and/or the assigned Single Point of Contact (SPOCO) to properly categorize DRs for validity, correctness of entries, accuracy and completeness of information and proper transmission of DRs to the proper Action Point.

5.9.2. The PM or PSM will establish a proactive process to analyze data and act accordingly to implement solutions to include the following specific objectives:

5.9.2.1. Correction of deficiencies is done within the program's available resources and prioritized by risk.

5.9.2.2. Identify and resolve T&E, product quality and materiel deficiencies throughout the system life cycle.

5.9.2.3. Commence deficiency reporting and resolution processes as early as possible, but not later than CDR. Early monitoring and oversight of system anomalies promotes the most effective technical and programmatic decisions for reducing total ownership cost.

5.9.2.4. Integrate deficiency analysis and resolution processes within quality, systems engineering and overall lifecycle management plans and documentation to identify root cause and prevent or mitigate recurrence.

5.9.2.5. Assess safety risks and investigate as necessary to resolve materiel deficiencies.

5.9.2.6. Provide historical collection of deficiency data to share knowledge with authorized activities responsible for design, development, safety, contracts and other related acquisition functional activities.

5.10. Risk Management Plans. The PM or PSM is required to prepare a Risk Management Plan (RMP) for all ACAT programs, potential ACAT programs, and Services Category I and II programs IAW AFI 63-101. The RMP describes the strategy by which the program will coordinate and integrate its risk management efforts to include a description and the responsibilities of the cross-functional risk management IPT.

5.10.1. The PM or PSM may be required to use the 5x5 risk matrix, likelihood criteria, and consequence criteria (IAW AFI 63-101) to assess cost, schedule, performance and other program risks including system safety. Per AFI 63-101, risks identified using the MIL-STD-882D system safety methodology shall be translated using Table 3.1 of AFI 63-101 (Table 5.1 below, Translation of MIL-STD-882D Risk Matrix to the OSD Risk Management Guide Matrix). All "High" and "Serious" ESOH risks identified using the MIL-STD-882D system safety methodology and the translation table will be presented by the PM or PSM as risk related information a part of all program technical, and Milestone decision reviews or to support other key decisions.

5.10.2. The SSM must be familiar with the MIL-STD-882D methodology, the translation of risk process IAW AFI 63-101 and how the identified system safety risks are factored in and related to the overall program risk management process.

5.10.3. Note that Tables A2.7 – A2.10 have been tailored to meet MIL-STD-882D or C mishap risk management methodology, applied to the SMC organization and hierarchy. Tables A.1.8 – A.1.11 will be used as the starting point for SMC government and RFP/contractual System Safety program tailoring. Variations will be coordinated in advance with appropriate authorities including SMC/SES, and shall be approved at appropriate levels in the SMC and higher level organizational hierarchy.

Table 5.1. Translation of MIL-STD-882D Risk Matrix to the OSD Risk Management Guide Matrix.

DoD Acquisition Risk Management Guide

LIKELIHOOD	1	2	3	4	5
5		IVA		IIA	IA
4		IVB	IIIA IIIB IIIC	IIB	IB
3		IVC	IIID IIIE	IIC	IC
2		IVD		IID IIE	ID
1		IVE			IE

CONSEQUENCE

MIL-STD-882D

PROBABILITY	IV	III	II	I
A				
B				
C				
D				
E				

SEVERITY

PAUL J. MEJASICH, GGE-15, DAFC
Director of Safety

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Table A1.1. Definition of Terms.

Terms	Definitions
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 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) Event	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 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 Analysis (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 or Systems Directorate. 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 Directorate or Program Office.
System Safety Management Plan (SSMP)	The SSMP is a document that contains guidance on how the Program Office or Directorate will implement System Safety requirements. When signed by both the Directorate or Program Office 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 and overall government organization's effort, meeting the same types of requirements as a 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/D, 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.

Table A1.2. Acronyms List.

ACAT	Acquisition Category
ADM	Acquisition Decision Memorandum
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
APB	Acquisition Program Baseline
APDP	Acquisition Professional Development Program
ASD	Acquisition Strategy Document
ARAR	Accident Risk Assessment Report
ASR	Alternative Systems Review
BS	Bachelor of Science degree
CARD	Cost Analysis Requirements Description
CAE	Component Acquisition Executive
CCA	Clinger-Cohen Act (CCA)
CCB	Configuration Control Board
CDD	Capabilities Development Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
COTS	Commercial Off The Shelf
CPD	Capability Production Document
CSOW	Contractor Statement of Work
CSP	Certified Safety Professional
CWBS	Contractor Work Breakdown Structure
DAL	Data Accession List
DID	Data Item Description
DoD	Department of Defense
DoDI	DoD Instruction
DOT	Department of Transportation
DR	Decision Review
ECP	Engineering Change Proposal
DRIS	Deficiency Reporting and Investigating System
EHC	Explosive Hazard Classification
EMD	Engineering & Manufacturing Development
EOLP	End-of-Life Plan
ESOH	Environment, Safety and Occupational Health
EWR	Eastern and Western Range
FCA	Functional Configuration Audit

FDP	Flight Data Package
FFRDC	Federally Funded Research and Development Corporation
FMECA	Failure Mode Effects and Criticality Analysis
FOC	Full Operational Capability
FRP	Full Rate Production
FRR	Flight Readiness Review
GFE	Government Furnished Equipment
GSE	Ground Support Equipment
GSOW	Government Statement of Work
HAP	High Accident Potential
HHAR	Health hazard Assessment Report
HMMPR	Hazardous Material Management Program Report
HRAM	Hazard Risk Assessment Matrix
HSI	Human Systems Integration
HSIP	Human Systems Integration Plan
IAW	In Accordance With
IBR	Integrated Baseline Review
ICD	Initial Capabilities Document, Interface Control Document
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IOC	Initial Operating Capability
IRRT	Independent Readiness Review Team
ISR	During Operations and Support In-Service Reviews
ITR	Initial Technical Review
LRIP	Low Rate Initial Production
MAJCOM	Major Command
MDD	Materiel Development Decision
MIL-STD	Military Standard
MRAM	Mishap Risk Assessment Matrix
MRAR	Mishap Risk Assessment Report
MRR	Mission Readiness Review
MS	Master of Science degree
MSA	Materiel Solution Analysis
MS-A	Milestone A
MS-B	Milestone B
MS-C	Milestone C
MSPSP	Missile System Pre-Launch Safety Package
NAVEODTECHCEN	Naval Explosive Ordnance Disposal Technology Center
NDI	Non-Developmental Item
O&S	Operations & Support
ORM	Operational Risk Management
O&SHA	Operating & Support Hazard Analysis

OSS&E	Operational Safety, Suitability, and Effectiveness
OT&E	Operational Test & Evaluation
OTRR	Operational Test Readiness Review
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
P&D	Production & Deployment
PEO	Program Executive Officer
PESHE	Programmatic Environment, Safety, & Occupational Health Evaluation
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager
PMB	Performance Measurement Baseline
PMR	Program Management Review
PRR	Production Readiness Review
PSM	Product Support Manager
RF	Radio Frequency
RFP	Request for Proposal
RFQ	Request for Quotation
SAE	Service Acquisition Executive
SAF	Secretary of the Air Force
SAR	Safety Assessment Report
SAF/AQ	Assistant Secretary of the Air Force for Acquisition
SAF/AQR	Deputy Assistant Secretary (Science, Technology and Engineering)
SAF/US	Under Secretary of the Air Force
SAR	Safety Assessment Report
SDAR	Space Debris Assessment Report
SDR	Systems Design Review
SEP	Systems Engineering Plan
SETA	Systems Engineering and Technical Assistance
SFR	System Functional Review
SFWC	Space Flight Worthiness Criteria
SMC	Space and Missile Systems Center
SMC/EN	SMC Engineering Directorate
SMC/ENF	SMC Enterprise Engineering Division
SMCI	Space and Missile Systems Center Instruction
SMC/SE	SMC Directorate of Safety
SMC/SES	SMC System Safety Division
SOW	Statement of Work
SRR	System Requirements Review
SSE	System Safety Engineer
SSG	System Safety Group
SHA	System Hazard Analysis

SSHA	Subsystem Hazard Analysis
SSHAR	System Safety Hazard Analysis Report
SSM	System Safety Manager
SSMP	System Safety Management Plan
SSO	System Safety Officer
SSPP	System Safety Program Plan
SSWG	System Safety Working Group
SVR	System Verification Review
TD	Technology Development
TDS	Technology Development Strategy
TES	Test and Evaluation Strategy
T&E	Test and Evaluation
TEMP	Test and Evaluation Master Plan
TRA	Technology Readiness Assessment
TRD	Technical Requirements Document
TRR	Test Readiness Review
TSRB	Test Safety Review Board
USD AT&L	Undersecretary of Defense for Acquisition, Technology, and logistics
WBS	Work Breakdown Structure

Attachment 2

APPLICABLE DOCUMENTS LIST

Table A2.1. Applicable Documents List.

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/
AFI 91-217, Space Safety And Mishap Prevention Program	Provides requirements for Space Debris and End-of-Life.	http://www.e-publishing.af.mil/
AFI 63-101, Acquisition And Sustainment Life Cycle Management	Translation of MIL-STD-882D Risk Matrix to the OSD Risk Management Guide Matrix.	http://www.e-publishing.af.mil/
AFI 91-110, Nuclear Safety Review And Launch Approval For Space Or Missile Use Of Radioactive Material And Nuclear Systems	Defines the nuclear safety review and launch approval procedures for using radioactive materials in space or missiles.	All versions can be found on the Web or from SMC/SE
AFI 63-1201, Life Cycle Systems Engineering		http://www.e-publishing.af.mil/
AFMAN 63-119, Certification Of System Readiness For Dedicated Operational Test And Evaluation	Defines PESHE requirements during operational tests.	http://www.e-publishing.af.mil/
AFMAN 99-103, Capabilities-Based Test And Evaluation		http://www.e-publishing.af.mil/
AFPD 91-2, Safety Programs, 28 September 1993	Air Force Safety Policy Directive	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/
AFSPCI 10-1204, Satellite Operations	Establishes guidance and procedures for satellite operations and disposal.	http://www.e-publishing.af.mil/
AFSPCI 10-604, Operations Space Operations Weapon System Management	Outlines Space Operations Weapon System Management processes of concept development, system development, acquisition, testing, and operations of Air Force Space Command (AFSPC) systems and equipment. Assigns roles and responsibilities of the planners, developers, operators, and maintainers, and describes the overall processes to conceive, develop, acquire, train, test, and transition a program or system providing space capabilities.	http://www.e-publishing.af.mil/
AFMAN 91-222, Space Safety Investigations and Reports		http://www.e-publishing.af.mil/
AFMAN 91-201, Explosives Safety Standards	Provides requirements for operations and facility siting involving explosives.	http://www.e-publishing.af.mil/
AFOSHSTD 48-9, Radio Frequency Radiation (RFR) Safety Program		http://www.e-publishing.af.mil/
AFOSHSTD 91-50, Communications Cable, Antenna And Communications-Electronic(C-E) Systems		http://www.e-publishing.af.mil/
AFOSHSTD 91-501, Air Force Consolidated Occupational Safety Standard		http://www.e-publishing.af.mil/
EWR 127-1, Eastern and Western Range, 31 October,	Used for legacy programs Only.	

1997		
DoDI 5000.02, Operation of the Defense Acquisition System, 08 December 2008	Guidance for DoD Space System Acquisition Process.	Can be found on the Web or from SMC/SE
DoDI 3100.12, Space Support, 14 September 2000	Guidance on Space Policy	Can be found on the Web or from SMC/SE
DoDD 3100.10, Space Policy, 09 July 1999	Guidance on Space Policy	Can be found on the Web or from SMC/SE
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
MIL-STD-882D, Department Of Defense Standard Practice For System Safety	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
ANSI/GEIA-STD-0010, Standard Best Practices for System Safety Program Development and Execution, 12 February 2009	Commercial Standard. Provides uniform requirements for developing and implementing a system safety program.	TechAmerica Standard
MIL-STD-1472F, Human Engineering	Guidance of safety, health and human factors engineering for equipment and facilities	All versions can be found on the Web or from SMC/SE
MIL-STD-1576, Electroexplosive Subsystem Safety Requirements and Test Methods For Space Systems		All versions can be found on the Web or from SMC/SE
MIL-STD-1522A, Standard General Requirements For Safe Design And Operation Of Pressurized Missile And Space Systems		All versions can be found on the Web or from SMC/SE

MIL-STD-1542B, Electromagnetic Compatibility And Grounding Requirements For Space System Facilities	Guidance for system safety design/grounding for space system facilities.	All versions can be found on the Web or from SMC/SE
MIL-STD-1540D, Product Verification Requirements For Launch, Upper Stage, And Space Vehicles		All versions can be found on the Web or from SMC/SE
MIL-HDBK 454B, General Guidelines For Electronic Equipment		All versions can be found on the Web or from SMC/SE
Software Safety Handbook	Funded and developed by the Joint Services Computer Resources Management Group, U.S. Navy, U.S. Army, and the U.S. Air Force Under the direction and guidance of the Joint Services Software Safety Committee of the Joint Services System Safety Panel and the Electronic Industries Association, G-48 Committee.	All versions can be found on the Web or from SMC/SE
29 CFR 1910, General Industry		All versions can be found on the Web or from SMC/SE
29 CFR 1926, Construction		All versions can be found on the Web or from SMC/SE
GIDEP (Government-Industry Data Exchange Program)	A cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production and operational phases of the life cycle of systems, facilities and equipment.	All versions can be found on the Web

SMC-S-015 (2008)	End-of-Life Disposal of Satellites Operating at Geosynchronous Altitude	Aerospace
SMC-S-001 (2008)	Systems Engineering	Aerospace
AEROSPACE REPORT NO. TOR-2008(8583)-8215, Space and Missile Systems Center Compliance Specifications and Standards		Aerospace
T.O. 00-35D-54, USAF Deficiency Reporting, Investigation, And Resolution	Provides the Air Force with a means of identifying deficiencies, resolving those deficiencies within the bounds of program resources and the appropriate acceptance of risk for those deficiencies that cannot be resolved in a timely manner.	All versions can be found on the Web or from SMC/SE

The Program Office or Systems Directorate 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 Systems Directorate SSMP. SMC/SES will work with Systems Directorate personnel in drafting the SSMP by providing additional samples and writing support.

Table A2.2. System Safety Management Plan Outline.

Government Systems Directorate/Division System Safety Management Plan (SSMP) Outline: TITLE PAGE SIGNATURE PAGE Revision History. CONTENTS CHAPTER 1: GENERAL 1.1. SSP Scope, Purpose and Objectives. 1.2. Reference key documents including SMCI 63-1205, and separate Systems Directorate System Safety operating instructions or SSG charters, if any. Reference appendices with terms,

reference documents, mishap risk management procedures.

CHAPTER 2: MANAGEMENT

2.1. System Safety and Systems Directorate organization.

2.2. Personnel authority and responsibility including Military, Civil Service, FFRDC, SETA and contractor.

2.3. Interfaces with other organizations including SMC System Safety Staff.

2.4. Interfaces and integration with other Systems Directorate processes including Risk Management, PESHE, OSS&E /Mission Assurance and Systems Engineering to ensure all necessary tasks are accomplished and none duplicated.

2.5. SSM direct access to program manager or product support manager.

2.6. SSM Functions in the Systems Directorate:

2.6.1. Systems Directorate point of contact for System Safety activities and consultation of behalf of the Systems Director.

2.6.2. Systems Directorate SSG, SSWG and Mishap Prevention/Risk Management. Government Systems Directorate/Division System Safety Management Plan (SSMP) Outline (continued):

2.6.3. SSM/SSE Design Drawing Review and Approval.

2.6.4. SSM membership in Systems Directorate's processes including CCB.

2.7. Task, Data, Schedule and Resource Requirements:

2.7.1. Schedule, manning and funding policy for tasks and data for all Systems Directorate programs in various phases.

2.7.2. Tasks including acquisition strategy participation, RFP development, proposal evaluation and source selection, Task Order & Plans development for FFRDC support, obtaining SETA support, etc.

2.7.3. Schedule.

2.7.4. Manning resources for Systems Directorate and programs including Military, Civil Service, FFRDC, SETA and contractor.

2.7.5. Funding.

2.8. Personnel Qualification Requirements (Education, Training, Experience, and Certification).

CHAPTER 3: SYSTEM SAFETY ENGINEERING

3.1. Areas of emphasis for system safety efforts.

3.2. List analyses and data needed (i.e., PHL, PHA, SSHA, SHA, O&SHA, SSPP, MRAR, etc.)

3.3. 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.

3.4. 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.

3.5. Specify participation in SSG/SSWG activities by Military, Civil Service, FFRDC, SETA and Contractor personnel. (See appendix for SSG Charter).

3.6. Schedule milestones and deadlines for system safety engineering tasks.

3.7. Draft schedule completion dates.

3.8. PHAs complete deadline, example 30 days before PDR.

3.9. SSHA complete deadline, example 30-45 days before CDR.
Government Systems Directorate/Division System Safety Management Plan (SSMP) Outline (continued):

3.10. SHA complete deadline, example 30-45 days before CDR.

3.11. O&SHA complete deadline, example 60 days before test or operation.

3.12. Other…

CHAPTER 4: SAFETY VERIFICATION AND OPERATION

4.1. Task safety engineering personnel to prepare and coordinate test plans and procedures.

4.1.1. Test Safety and Test Safety Review Board.

4.1.2. Safety Tests.

4.2. Operational and Space Safety.

4.2.1. System Safety roles and responsibilities in Systems Directorate and Program OSS&E.

4.2.1.1. Space Flight Worthiness Criteria.

4.2.1.2. Independent Readiness Review Team.

4.2.2. 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 Systems Directorate and higher processes, …).

4.2.3. Provide requirements for qualified people to accomplish the tasks (Weapons Safety training, Space Safety training, Orbital Safety Officers, …)

4.2.4. Establish authority for implementing tasks through all levels.

4.2.5. 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 Systems Directorate programs' System Safety processes.

CHAPTER 5: OTHER/SPECIAL TOPICS

5.1. 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.

Table A2.3. 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"

Table A2.4. 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 …"

Table A2.5. Preliminary Hazard Analysis.

1. Subsystem/Operation: TT&C.
2. Mission Phase: Pre-Launch Tests and Processing.

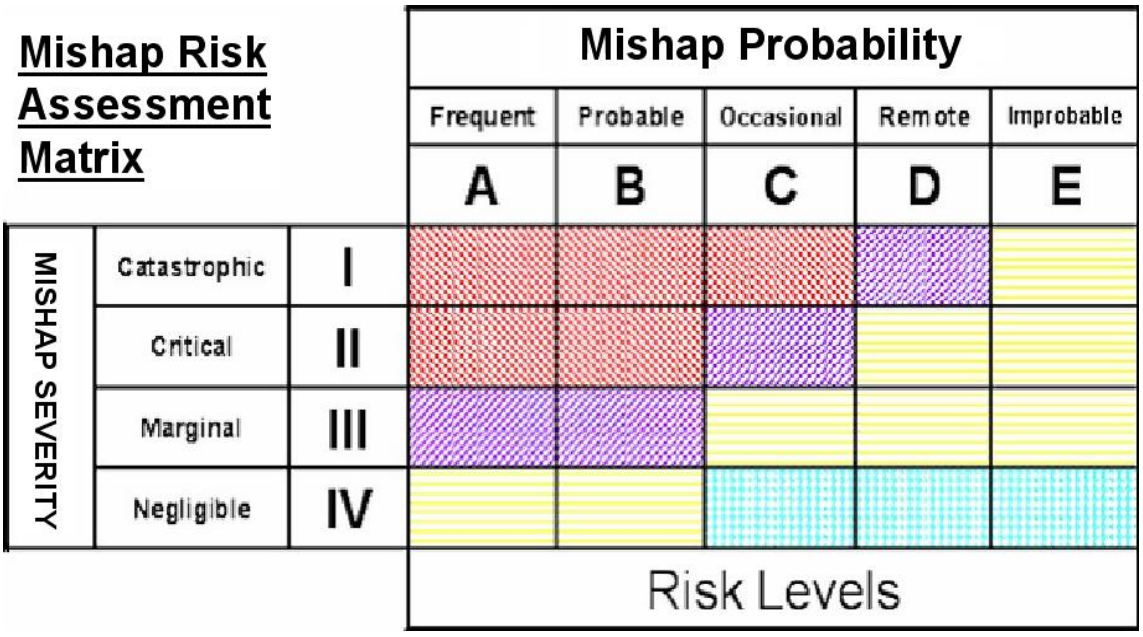
Hazard Cause	Hazard Level /Effect	Safety Requirements	Hazard Control	Verification	Status
1. RF energy exceed allowable personnel limits for planned ground and pre-launch operations.	1. Critical – Personnel Injury	1. *AFSPCMAN 91-710 V3,* Para. 8.1.1.1, Radio Frequency Emitters shall be designed to ensure that personnel are not exposed to hazardous energy levels in accordance with ANSI/IEEE C95.1, *Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields.*	1. Testing and maintenance of RF emitters is accomplished 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 ANSI/IEEE C95.1.	1. Review of drawings, RF hat attenuation analysis, test, and procedures.	1. Open

Table A2.6. Hazard Control Report Form (Sample).

SMC/SES System Safety Program	HAZARD REPORT	Hazard Report Number:_____ 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)	

Table A2.7. Mishap Risk Assessment Matrix.



Mishap Risk Acceptance. The Mishap Risk Assessment Matrix (Table A2.7) above contains mishap 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 mishap 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 Systems Directorate and their 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 mishap risk 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 mishap probability to a potential design or procedural mishap risk is generally not possible early in the design process. A qualitative mishap risk probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability shall be documented in hazard analysis reports.

As hazards are identified and assessed, it is important to make sure they enter the program risk management process where mitigation plans would be tracked and monitored. The Probability and Severity assessment should be mapped to the standard risk assessment criteria of Likelihood and Consequence. (Possibly there would be a mapping for each hazard, rather than a single mapping that applies to all hazards in the program.) Typically, hazard mitigation would have impact on schedule and cost, so in the risk management process, a safety risk should appear as a schedule and/or cost risk.

Table A2.8. Mishap Probability Definition.

Mishap Probability Definition	
Frequent	Likely to occur frequently in life of system, item, facility, etc. Continuously experienced in fleet/ inventory. Probability of Occurrence: X) > 10-1
Probable	Will occur several times in life of item. Will occur frequently in fleet/inventory. Probability of Occurrence: 10-1 > (X) > 10-2
Occasional	Likely to occur sometime in life of item. Will occur several times in fleet/inventory. Probability of Occurrence 10-2 > (X) > 10-3
Remote	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
Improbable	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)

Table A2.9. Mishap Severity Definition.

Mishap Severity Definition	
Catastrophic	Death or permanent total disability, system loss, major property damage, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	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.
Marginal	Minor injury, lost workday accident, or compensable injury/illness; minor system or property damage, loss exceeding $10K but less than $200K, or mitigable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	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.

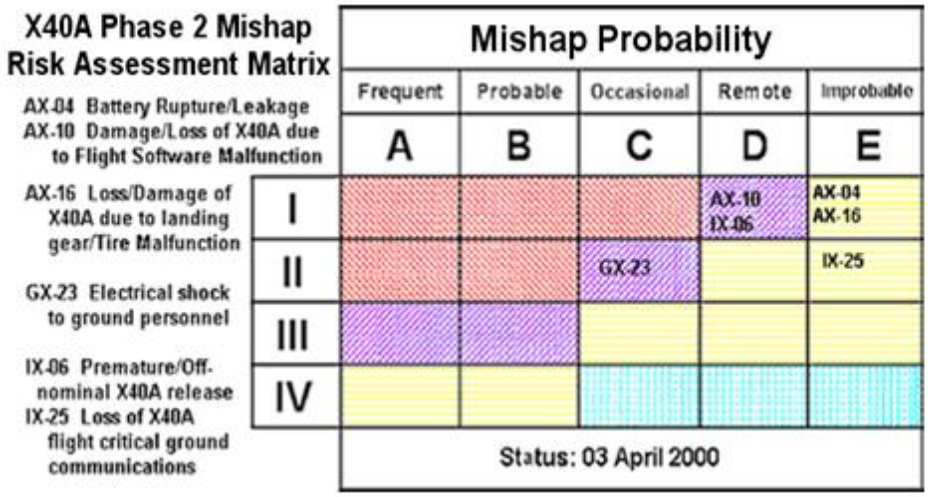
Table A2.10. Mishap Risk Acceptance Matrix.

Mishap Risk Acceptance Matrix

Residual Mishap Risk Assessment Value	Mishap Risk Category	Mishap 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) or Product Support Manager (PSM)
IVC, IVD, IVE	Low	SSM/Chief Engineer Summary to PM or PSM

The above chart (Table A2.10) was created by SMC/SES to help the user assign risk to the appropriate residual risk acceptance authority for SMC programs and projects. It has a direct correlation to the Mishap Risk Assessment Matrix above for severity, probability and risk.

Table A2.11. Mishap Risk Assessment Matrix (NASA Sample).



The above chart is an example of the Mishap Risk Assessment Matrix from the NASA X40A Phase 2 acquisition program.

Table A2.12. Example Tailored MIL-STD-882C Task Lists: Satellite/Launch Vehicle (Ref. for programs applying MIL-STD-882C).

Example Tailored MIL-STD-882C Task List: Satellite/Launch Vehicle	
Task	Tailoring
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 Systems Directorate.
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 (DAL) and be accessible to the government.
Task 107 (System Safety Progress Summary)	Prepare quarterly system safety reports as part of the Systems Directorate's Quarterly Review.
Task 201 (PHL).	The contractor shall begin preparing the list NLT shortly after MS-A approval. 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 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 the Systems Directorate within one working day of identifying the change in the hazard severity or probability by one level or greater.
Task 401 (Safety Verification).	All.
Task 403 (EHC Data).	Tailor 403.2.1 to include only the AF Explosive Hazard Classification Procedures. Delete 403.2.1.2.

Table A2.13. Example Tailored MIL-STD-882C Task List: Ground System (Ref. for programs applying MIL-STD-882C).

Example Tailored MIL-STD-882C Task List: Ground System	
Task	Tailoring
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 Systems Directorate.
Task 103 (Integration of Associate Contractors, Subcontractors and A&E Firms). (Assume prime and subcontractors).	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 (DAL) and be accessible to the government.
Task 107 (System Safety Progress Summary)	Prepare quarterly system safety reports as part of the Systems Directorate's Quarterly Review.
Task 201 (PHL).	The contractor shall begin preparing the list NLT shortly after MS-A approval. 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 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 the Systems Directorate within one working day of identifying the change in the hazard severity or probability by one level.
Task 401 (Safety Verification).	All

Table A2.14. Contractor Data Requirements Lists (CDRLs).

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 Systems Directorate's SSM and 1 copy to SMC/SE
Mishap Risk Assessment Report Part A: MSPSP/other range requirements. Tailor MSPSP to AFSPCMAN 91-710 requirements. Part B: other than range requirements for entire life cycle.	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 Systems Directorate's SSM, 1 copy to SMC/SE, 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 Systems Directorate's SSM and 1 copy to SMC/SE (same as for satellite/launch vehicle program)
Safety Assessment Report (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 Systems Directorate's SSM and 1 copy to SMC/SE.

Table A2.15. Data Item Descriptions (DID) List and Data Accession List (DAL).

DID Number	DID Title
DI-SAFT-81626	System Safety Program Plan (SSPP)
DI-SAFT-80101B	System Safety Hazard Analysis Report
DI-SAFT-80102B	Safety Assessment Report
DI-SAFT-80103B	Engineering Change Proposal System Safety Report
DI-SAFT-80104B	Waiver or Deviation System Safety Report
DI-SAFT-80105B	System Safety Program Progress Report
DI-SAFT-80106B	Health Hazard Assessment Report
DI-MISC-80508B	Technical Report – Study/Services
DI-SAFT-80931B	Explosive Ordnance Disposal Data
DI-SAFT-81065	Safety Studies Report
DI-SAFT-81066	Safety Studies Plan
DI-ADMN-81250A	Conference Minutes
DI-SAFT-81299B	Explosive Hazard Classification Data
DI-SAFT-81300A	Mishap Risk Assessment Report
DI-ILSS-81495	Failure Mode Effects, and Criticality Analysis Report

Table A2.16. Data Item Descriptions And MIL-STD-882C Tasks Matrix (Ref. for programs applying MIL-STD-882C).

DID No.	DID Description	Tasks Supported
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 Ordnance 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

Table A2.17. MIL-STD-882C Tasks and Data Item Descriptions Matrix. (Ref. for programs applying MIL-STD-882C).

Task Description	DID No.	DID Description
101 - System Safety Program	DI-SAFT-80100A	System Safety Program Plan
102 - System Safety Program Plan	DI-SAFT-80100A	System Safety Program Plan

103 - Integration/Management of Associate Contractors, Subcontractors, and Architect and Engineering Firms	DI-SAFT-80100A	System Safety Program Plan
104 - System Safety Program Reviews/ Audits	DI-SAFT-80105A	System Safety Program Progress Report
105 -System Safety Group/System Safety Working Group Support	As per CDRL	As per CDRL
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	As per CDRL	As per CDRL

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
Mishap Risk Assessment (App. A, Para 50.5)	DI-SAFT-81300	Mishap Risk Assessment Report