System Safety Implementation Plan for

the Goddard Space Flight Center

Explorers Program Office

410-PLAN-0068
Rev. A

May 10, 2005

SIGNATURE PAGE

Prepared By: _____ Date: 5-27-05
James Burget
EXP Program Safety Engineer

Reviewed By: _____ Date: 5/27/05
James T. Harper
EXP Program Safety Manager

Reviewed By: _____ Date: 5/27/05
Ronald E. Perison
EXP Systems Assurance Manager

Approved By: _____ Date: 5/27/05
Anthony B. Comberiate
Associate Director/Program Manager for EXP

DOCUMENT CHANGE RECORD

REVISION	DESCRIPTION	DATE	APPROVAL
-	Initial Release	12/2/04	
A	- Revised obsolete document references - Incorporated new GSFC safety requirements	5/10/05	

ABBREVIATIONS AND ACRONYMS

AFSPCMAN	Air Force Space Command Manual
CDR	Critical Design Review
CDRL	Contract Deliverable Requirements List
EXP	Explorers
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
KSC	Kennedy Space Center
LSP	Launch Services Program
MAG	Mission Assurance Guidelines
MAR	Mission Assurance Requirements
MSPSP	Missile Systems Prelaunch Safety Package
NASA	National Aeronautics and Space Administration
NPR	NASA Procedural Requirements
OHA	Operations Hazard Analysis
OSHA	Occupational Safety and Health Administration
PER	Pre-Environmental Review
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PSM	Program Safety Manager
SAM	Systems Assurance Manager
SMAO	Safety and Mission Assurance Office
SSIP	System Safety Implementation Plan
VTL	Verification Tracking Log

TABLE OF CONTENTS

TABLES

1.0 INTRODUCTION

This document establishes the overall System Safety Implementation Plan (SSIP) for the Goddard Space Flight Center (GSFC) Explorers (EXP) Program. It describes the safety approach that will be followed during the design, development, fabrication, assembly, and test phases of mission hardware from conception through launch.

1.1 Purpose

The purpose of the system safety program is to assure safe design and operation of payloads so that personnel, equipment, the launch vehicle, and facilities are protected against hazardous conditions. This document provides guidelines for managing safety hazards throughout the ground portion of the mission up to launch.

1.2 Scope

This SSIP encompasses the activities required for satisfying and demonstrating compliance with all safety requirements that apply to the design, fabrication, assembly, handling, transportation, verification, integration, and ground operations phases of the mission elements. This plan outlines the approach and the responsibilities of organizational elements within EXP for implementing the system safety program.

1.3 Applicability

This document applies to all persons, organizations, governments, and contractors that are engaged in providing hardware or software, including Ground Support Equipment (GSE) or conducting operations under the cognizance of EXP.

1.4 Applicable and Referenced Documents

The following documents are applicable to all missions to the extent specified in each contract:

29 CFR 1910	Occupational Safety and Health Standards
300-PG-7120.2.2D	Mission Assurance Guidelines (MAG) for Tailoring to the Needs of GSFC Projects
AFSPCMAN 91-710	Range Safety User Requirements
KNPR 8715.3	KSC Safety Practices Procedural Requirements
NPR 8715.3	NASA Safety Manual
NPR 8621.1	NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping

The following document is applicable to all missions as referenced material:

NASA-STD-8719.8 Expendable Launch Vehicle Payload Safety Review Process

Other documents may be specified by individual contract and/or those documents listed as applicable in the above section.

2.0 SYSTEM SAFETY PROGRAM IMPLEMENTATION

2.1 System Safety

Each organization involved shall institute a rigorous system safety program beginning with the conceptual phase of the element. System safety requirements shall be an integral part of all technical developments. Management controls shall be devised for effective and efficient implementation of this plan. A SSIP shall be written and submitted to EXP by each mission project organization to demonstrate how the project will comply with the requirements of AFSPCMAN 91-710, NPR 8715.3, and KNPR 8715.3, and has a instituted comprehensive system safety program (refer to Section 5.1 for further SSIP information).

2.2 Contractual Implementation

Procurements for integration, software, support equipment and personnel support shall include requirements for system safety. The specific requirements shall be compatible with the content and intent of this document. The scope and detail of the system safety effort shall be sized for optimum effectiveness and shall be consistent with this document.

Safety deliverables, as required by AFSPCMAN 91-710 and 300-PG-7120.2.2D and specified in the Mission Assurance Requirements (MAR) and Contract Data Requirements List (CDRL) shall be prepared by the project and submitted to EXP for approval. Once approved, the EXP Office will forward all deliverables to the Kennedy Space Center (KSC) Launch Services Program (LSP) for distribution to Range Safety and the KSC Safety and Mission Assurance Office (SMAO).

2.3 Industrial Safety and Health

Industrial safety and health is incorporated into every phase of the operation. All accidents and incidents shall be reported per OSHA requirements. Those of significance to the payload shall also be reported to the EXP Office.

Elements involving hazardous commodities shall be analyzed and monitored by environmental health personnel to assure personnel are not exposed to dangerous conditions.

2.4 General Safety Guidelines and Requirements

Every person involved in an EXP mission is responsible for safety. Individual personnel are responsible for adherence to safety requirements, for the implementation of good practices and techniques, and for reporting to their supervisor any condition, existing or anticipated, that they consider hazardous. Good safety practices must always come first in any project. As a general rule, all OSHA and State safety regulations must be followed, as well as those of NPR 8715.3, NASA Safety Manual. If there is a conflict between OSHA, State and/or NASA requirements, the most stringent will always be followed.

3.0 ORGANIZATION AND RESPONSIBILITIES

3.1 Organization

EXP is under the overall management of NASA GSFC. The EXP Office provides mission management services and serves as NASA's range user representative. All organizations that make-up an EXP mission are responsible for assuring the safe design of their flight hardware and GSE, as well as its safe operation. As the range user, NASA/EXP is responsible for assuring that all payload elements are compliant with applicable safety requirements, as well as certifying that the interaction of all payload elements does not create a hazard.

3.2 EXP Associate Director/Program Manager

As the NASA range user representative, the EXP Associate Director/Program Manager has overall responsibility for the launch vehicle payload. The Associate Director/Program Manager, or designated Mission Manager, ensures the Payload Project Manager institutes a formal system safety program in accordance with AFSPCMAN 91-710 and NPR 8715.3. The Associate Director/Program Manager ensures the Payload Project Manager formally considers all residual risks and agrees to their acceptance.

The Associate Director/Program Manager will inform GSFC Management of decisions involving the acceptance of significant residual risks that remain after all practical steps have been taken to reduce hazards. The Associate Director/Program Manager will have sufficient resources to carry out this plan and ensure that safety provisions are included in project procurements.

The Associate Director/Program Manager, or designated Mission Manager, will approve all safety deliverables prior to submittal to Range Safety and the KSC SMAO via the KSC LSP.

3.3 EXP Program Safety Manager Responsibilities

The EXP Program Safety Manager (PSM) disseminates EXP safety policies/requirements and other applicable safety policies and requirements established by NASA Headquarters, GSFC, KSC, and Range Safety. The PSM monitors the project's system safety program for compliance with these requirements and reviews safety packages, establishment of Safety Working Groups and compliance verification activities. As required, the PSM will coordinate project system safety matters with other government agencies and contractors.

The PSM is available, upon request, to all hardware developers to consult on system safety requirements and implementation.

The PSM has the overall responsibility for implementing this SSIP, in support of EXP. The PSM will ensure that the payload verification plans include the tests, inspections, and analyses that are necessary for demonstrating compliance with applicable safety requirements.

The PSM will receive all required technical documentation and verify its completeness. Utilizing the technical documentation, the PSM will prepare the payload safety certification letter.

3.4 Other Involved Groups' Responsibilities

All persons, organizations, and contractors are responsible for compliance with the appropriate safety related documents, as called out in their contracts. They shall provide an effective safety program for their personnel, as well as other organizational personnel involved in their operations. They will provide all necessary safety related documentation to the project to assure a comprehensive safety approach has been implemented into their organization and operations. The project shall require safety data packages to document compliance with the safety requirements of AFSPCMAN 91-710. Supporting documentation such as analysis and/or test reports necessary to verify the adequacy of hazard controls or compliance with specific safety requirements shall also be provided.

4.0 SYSTEM SAFETY CRITERIA

4.1 Hazard Severity Categories

Hazard severity categories will be used to provide a qualitative measure of the worst credible mishap resulting from personnel error, design inadequacies, environmental conditions, procedural deficiencies or systematic failures or malfunctions. Hazard severity categories, as defined in NPR 8715.3, are as follows:

A. Class I - Catastrophic: Death or permanently disabling injury, or facility destruction, or loss of system and/or vehicle

B. Class II - Critical: Severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware

C. Class III - Moderate: Minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware

D. Class IV - Negligible: Minor first aid treatment that would not adversely affect personal safety or health, or condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear

4.2 Safety Design Requirements

If a system failure may lead to a **catastrophic hazard**, the system shall have three independent, verifiable inhibits (dual fault tolerant).

If a system failure may lead to a **critical hazard**, the system shall have two independent, verifiable inhibits (single fault tolerant).

Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" areas. These areas have separate, detailed safety requirements that must be met. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.

4.2.1 Additional Safety Design Considerations

The following design considerations shall be used, as applicable, to perform hazard analyses on hardware and its interfaces and will be considered satisfactory design resolutions to identified hazards. Satisfactory resolutions include:

A. System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause an accident.

B. System designs that positively prevent errors in assembly, installation or a connection, which could result in an accident.

C. System design limitations on operation, interaction or sequencing, which preclude occurrence of an accident.

D. System designs that provide an approved safety factor or fixed design allowance which minimizes possibilities of structural failure or release of energy sufficient to cause an accident.

E. System designs that control energy buildup which could potentially cause an accident (fuses, pressure relief, electrical explosion proofing, etc.)

F. 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. The assumptions made to reach the conclusion of "temporarily tolerated failure" shall be documented.

G. System designs that positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been proved.

H. System designs that minimize/control the use of flammable materials.

4.3 System Safety Precedence

Actions for satisfying safety requirements and criteria, in order of precedence will be implemented as follows:

A. Hazard Elimination--The primary effort throughout design and development will be to select and incorporate appropriate safety features. This effort includes such considerations as fail-safe operation, redundancy, protective devices, material control and energy-transfer control.

B. Safety Devices--Appropriate safety devices will be incorporated to control or reduce hazards to an acceptable level when identified hazards cannot be eliminated through design. Safety devices include such items as pressure-relief valves, voltage or current limiters, isolators and shields.

C. Protective Systems--Where accident risks cannot be totally eliminated, the employment of systems to prevent injury to personnel, equipment or property is acceptable risk reduction. Such systems include fire suppression, radiation shields, blast shields, etc.

D. Warning Devices--Where it is not possible to preclude the existence or occurrence of an identifiable hazard, devices will be employed for its timely detection and the generation of an adequate warning signal. These warning signals will be designed to ensure correct and appropriate personnel reaction. Typical primary warning devices are visual displays or audible signals activated by mechanical, chemical or electrical energy when pre-set limits are exceeded. Examples of such devices are indicator-type fuses, high or low temperature monitors, high or low-pressure monitors, etc.

E. Special Procedures--Special procedures will be developed wherever it is not possible to reduce the magnitude or probability of an existing or potential hazard by means of efforts and devices.

5.0 SYSTEM SAFETY DELIVERABLES

5.1 System Safety Implementation Plan

A System Safety Implementation Plan (SSIP) shall be completed to provide a formal basis of understanding of how the mission System Safety program will be conducted to meet the requirements of AFSPCMAN 91-710, NPR 8715.3, and KNPR 8715.3. The SSIP describes in details the systems safety management and engineering tasks and activities required to identify, evaluate, and eliminate or control hazards by reducing the associated risk throughout the system lifecycle. The Final Mission SSIP shall be submitted to EXP for approval no later than the Mission Preliminary Design Review (PDR).

5.2 AFSPCMAN 91-710 Tailoring

AFSPCMAN 91-710 tailoring shall be completed for all design, test, analysis, and data submittal requirements to identify whether the proposed design is complaint, non-compliant but meets an equivalent level of safety, non-compliant and requires a waiver, or not applicable.

Final AFSPCMAN 91-710 tailoring shall be submitted to EXP for approval no later than the Mission PDR. Once all issues and concerns are resolved, the EXP Office will submit the AFSPCMAN 91-710 to the KSC LSP for distribution to Range Safety and the KSC SMAO.

5.3 System Safety Analysis

The project system safety representative shall perform a managed, disciplined and continuous process of qualitative system safety analysis of the mission payload, GSE, operations, and associated interfaces. The purpose of the process is to ensure the early identification of accident risk and to initiate a controlled and managed system of risk reduction. The results of this analysis will be assessed for adequacy of hazard controls and verification methods and will be summarized for inclusion in the MSPSP. The analysis will be performed by the system safety representative who will (with the assistance of the cognizant experiment/subsystem engineering personnel):

A. Conduct (or require the conduct of) an analysis of the hardware and associated interfaces, including subcontracted elements.

B. Develop the files, records, reports and controls necessary to surface and react to all identified accident risks.

C. Ensure the control and documentation of each identified risk requiring waiver approval.

D. Ensure that the analysis is conducted as an iterative process throughout the program so that changes to the initial configuration of the hardware and interfaces are accommodated, and that experience gained during build, test and operational phases is included and thoroughly assessed for risk.

The status of this system safety effort shall be part of all subsystem presentations during project design reviews.

5.3.1 Preliminary Hazard Analysis

A Preliminary Hazard Analysis (PHA) shall be conducted to the subsystem and critical operational level for the payload. The purpose of the PHA is to provide an initial assessment of the safety-critical aspects of the design and to identify the potential risk factors. Design and procedural controls will be identified to eliminate or minimize hazards to an acceptable level. Areas requiring subsequent detailed analysis will be identified, as well as potential hazard groups associated with each subsystem component. The PHA shall be completed and submitted to EXP for approval no later than 45 days prior to Mission PDR.

5.3.2 Operations Hazard Analysis

An Operations Hazard Analysis (OHA) shall be completed to evaluate the flight hardware and test equipment operations to determine if the planned Integration and Test (I&T) activities are compatible with facility safety requirements. Any inherent hazards associated with those activities are then mitigated to a level acceptable to project management. The Final OHA shall be submitted to EXP no later than 45 days prior to the observatory CDR.

5.3.3 Final Integrated Hazard Analysis

A final integrated hazard analysis shall be conducted to the subsystem and critical operations level for the payload and associated GSE and shall be based on the system descriptions and safety assessment reports. The purpose of this analysis is to provide a final assessment of the safety critical aspects of the design and to identify the potential risk factors. This analysis will be included as part of the MSPSP.

5.4 Missile Systems Prelaunch Safety Package

A Missile Systems Prelaunch Safety Package (MSPSP) will be prepared to address hazards associated with the payload and associated GSE based on applicable AFSPCMAN 91-710 requirements. The MSPSP provides detailed descriptions of the payload and GSE designs, systems, and materials, as well as hazardous and safety critical operations associated with the payload. The MSPSP identifies hazards, indicates actions taken to eliminate or control hazards, and provides rationale for risk acceptance. Hazard Reports will be required as part of the MSPSP in establishing a “closed loop” process for tracking all hazards to acceptable closure.

Three MSPSP submissions (Preliminary, Intermediate, and Final) will be prepared by the project and delivered to EXP for review and approval. Once all issues and concerns are resolved, the EXP Office will submit the MSPSP to the KSC LSP for distribution to Range Safety and the KSC SMAO. Table 5.4 details the MSPSP submittal schedule to Range Safety/KSC.

Table 5.4 MSPSP Submittal Schedule

MSPSP Submission	Due date to Range Safety/KSC (via EXP)
Preliminary MSPSP	Mission PDR +30 days
Intermediate MSPSP	Mission CDR + 30 Days
Final MSPSP	No later than 60 days prior to shipment to the Range

5.4.1 Hazard Reports and Verification Tracking Log

Hazard Reports will be required as part of the MSPSP to identify applicable hazard controls, verifications, and tracking methods for each hazard of catastrophic or critical severity. Hazard Reports shall be broken down per subsystem and hazard group and will include a description of the hazard, potential causes, hazard controls, hazard control verification methods, and verification status. Reference Appendix A for the recommended Hazard Report format.

A Verification Tracking Log (VTL) shall be utilized to track all items requiring verification as identified in the Hazard Reports. An initial VTL shall be established upon EXP acceptance of the Intermediate MSPSP. The recommended VTL format is located in Appendix B.

5.5 Safety Noncompliance Reports (Waivers)

Any identified unresolved issues that do not meet NASA or AFSPCMAN 91-710 requirements will be addressed by the preparation of Safety Noncompliance Reports (waivers). The waiver request will be prepared by the project and submitted to EXP for approval. The project will be responsible for submitting a request that identifies the hazard and specific safety requirement noncompliance and shows rationale for approval. All approved safety waivers will be documented in the MSPSP and subsequently addressed in the safety approval process for ground operations, readiness reviews, and launch.

6.0 ACCIDENT/INCIDENT (MISHAP) INVESTIGATION AND REPORTING

Accident/incident investigation and reporting on NASA equipment and/or personnel will be investigated and reported in compliance with NPR 8621.1 “NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping”.

All incidents will be reported to the EXP Office and the EXP PSM within 24 hours and a formal report will be submitted within 10 days. Safety related failures or mishaps occurring prior to arrival at the launch site shall be reported at safety review meetings.

Appendix A

Sample EXP Hazard Report Form

PROJECT HAZARD REPORT		a. NO:
b. PROJECT:		
c. SUBSYSTEM:	d. HAZARD GROUP:	e. DATE:
f. HAZARD TITLE:		g. HAZARD CATEGORY ☐ CATASTROPHIC ☐ CRITICAL
h. APPLICABLE SAFETY REQUIREMENTS:		
i. DESCRIPTION OF HAZARD:		
j. HAZARD CAUSES:		
k. HAZARD CONTROLS:		
l. SAFETY VERIFICATION METHODS:		
m. STATUS OF VERIFICATION:		

n. APPROVAL	PROJECT MANAGER	EXPLORERS PROGRAM
PRELIMINARY		
FINAL		

EXP Hazard Report Form

PROJECT HAZARD REPORT CONTINUATION SHEET	a. NO:
b. PROJECT:	
j. HAZARD CAUSES:	
k. HAZARD CONTROLS:	
l. SAFETY VERIFICATION METHODS:	
m. STATUS OF VERIFICATION:	

Instructions for the completion of the EXP Hazard Report Form

a. NO: Insert a unique alphanumeric designation that will be used to track the hazard report. These designations will be assigned by the project when the report is first submitted and must be retained for all future updates of the hazard report.

b. PROJECT: Insert the name of the project.

c. SUBSYSTEM: Enter applicable observatory/GSE subsystem.

d. HAZARD GROUP: Identify the credible result of the hazard (i.e. fire, electrical shock, explosion, collision, temperature extremes, radiation, etc.).

e. DATE: Insert the date completed or revised.

f. HAZARD TITLE: The title should include a brief descriptive reference of the hazard to be addressed in the hazard report.

g. HAZARD CATEGORY: Mark the appropriate block (critical or catastrophic) using the definitions included in NPR 8715.3.

h. APPLICABLE SAFETY REQUIREMENT: Indicate the applicable paragraph number of the current version of AFSPCMAN 91-710 “Range Safety User Requirements” technical requirements related to the identified hazard.

i. DESCRIPTION OF HAZARD: The scope of hazards to be reported includes those related to the following: personnel injury or death; damage to or loss of the spacecraft, ground facilities, or equipment; or the use of contingency or emergency operations by ground personnel. The hazard description should define the risk situation including the unsafe act or condition and its effect on the spacecraft or personnel.

NOTE: The order of precedence for reducing hazards is defined in NPR 8715.3, Section 3.4

j. HAZARD CAUSES: Itemize the identified causes for the risk situation and the unsafe act or condition listed under the hazard description. Among hazard causes may be the environment, personnel error, design characteristics, procedural deficiencies, or subsystem malfunctions.

k. HAZARD CONTROLS: Completed for the preliminary MSPSP submittal and updated as required for subsequent safety data submittal(s). Clearly show a direct correlation between each hazard cause and the corresponding hazard control(s).

- Identify the design features, safety devices, warning devices, and/or special procedures that will eliminate, reduce, safe, or counter the hazards resulting from each cause.
- Identify any procedures or processes in manufacturing or assembly that are critical in controlling hazards.
- Attach to the HR sufficient detailed supporting information for each control, including data from the Missile Systems Prelaunch Safety Package (MSPSP) system description and operations if that data is necessary to clarify details concerning the control.

l. SAFETY VERIFICATION METHODS: Identify the safety verification methods used to assure the validity of the hazard controls. A direct correlation between each verification method and the corresponding hazard control must be clearly shown on the hazard report. Where procedures/processes in manufacturing or assembly are critical elements in controlling hazards and where the results cannot or will not be verified by subsequent inspection or test, it is mandatory to insure that the procedure/process is adequate for the purpose and that the steps of the procedure/process are verified as they occur. The responsible project element(s) shall be stipulated for each verification.

An independent verifier shall attest to proper completion of the procedure/process.

- For the preliminary submittal, this block should include the types of tests, analyses, or procedures (i.e. vibration testing) to be used to verify each hazard control, including all project provided services or interfaces for each verification which stipulate the responsible project sub-element. This block should be updated as appropriate to refer to specific test (or analysis) procedures and a summary of criteria to be used.
- For the final submittal, all safety verifications should be completed, and this block should be updated to reflect any changes in the verification methods made after the preliminary submittal.

m. STATUS OF VERIFICATION: Indicate the status (open, closed, or closed to the VTL) of each safety verification. Each status item will be identified by the same number as the verification method item to which it is related.

- For the preliminary submittal, provide a tentative schedule for completion of each specific verification test, analysis, or inspection.
- For final submittal, this block should summarize the results of the completed tests, analyses, and/or inspections and refer to particular test reports by document number and title. All safety verifications that are still incomplete at final submittal must be indicated as “closed to the VTL” on the hazard report.

n. APPROVAL: Project Management and EXP must sign and date the hazard report for the appropriate submittal. A copy of this signed form must be included in the corresponding MSPSP. Original signed hazard reports must be submitted to the EXP Mission Manager after acceptance.

Appendix B

Sample EXP Verification Tracking Log (VTL) Format

LOG #	HAZARD REPORT #	SAFETY VERIF. #	DESCRIPTION	GROUND OPERATIONS CONSTRAINED	INDEPENDENT VERIFICATION REQUIRED	APPLICABILITY	SCHEDULED DATE	COMPLETED DATE	COMMENTS
1									
2									
3									
4									
5									
6									
7									
8									