Gravity Probe B Relativity Mission
System Safety Program Plan

_____
Prepared by: Phil Unterreiner, Quality Engineering

_____
Approved by: B. Taller, System Effectiveness Manager

_____
Approved by: John Turneaure, Hardware Manage

_____
Approved by: Brad Parkinson, Program Manager

_____
Approved by: Lawrence Gibbs, Stanford Environmental Health & Safety

1.0 GENERAL

1.1 Introduction

This document presents the System Safety Program Plan (SSPP) for the Gravity Probe B (GP-B) Relativity Mission experiment being developed by the Stanford University (SU) for the National Aeronautics and Space Administration (NASA). This Plan will assist SU in developing, implementing, and managing a formal System Safety Program (SPP) for the GP-B Program that will meet NASA Marshall Space Flight Center (MSFC) requirements as well as the Eastern and Western Range Safety Requirements.

1.2 Background

Stanford University is the prime contractor to NASA for the GP-B Program. The objective of the Program is to design, develop, and conduct a flight experiment that will test two areas of Albert Einstein's General Relativity Theory. The General Relativity Theory is the basis of our current understanding of the large-scale structure of the Universe, but is difficult to reconcile with other aspects of modern physics and is strongly in need of additional testing. The Relativity Mission will use ultraprecise gyroscopes in space to measure two phenomena, the geodetic effect and the frame-dragging effect, in an effort to prove or disprove Einstein's theory.

The GP-B Program is very complex and potentially hazardous. This is due to a variety of activities involving the development, handling, transportation, and launch of the payload and space vehicle. Additionally, a major component of the payload is a large dewar containing nearly 2300 liters of liquid helium; an inherently hazardous substance requiring special handling and safeguards. Therefore, it is important to recognize that throughout this Plan, any reference to the GP-B SSPP will include consideration of environmental health and safety (EH&S), industrial hygiene, and operational, industrial, and system safety concerns.

1.3 Scope and Purpose

This SSPP is developed using MIL-STD-882C, Task 102, as a guide, but tailored to the specific needs of the GP-B Program. This Plan is a management tool which establishes management policies and objectives for the execution of the GP-B Program SSPP and describes SSPP organizational responsibilities, system safety methodologies, procedures to verity the achievement of safety objectives, program milestones, integration with other GP-B Program activities, and procedures for evaluating safety program performance.

This SP meets GP-B Program system safety requirements and delineates the necessary tasks required to ensure the achievement of all safety requirements. Also presented herein are the areas of responsibility for meeting various safety requirements, as well as meeting program schedules and interfacing with other functional disciplines. This Plan will be updated, as required, by changes in the program, procedures, or requirements. The updating effort will continue throughout the life of the program in a controlled and systematic manner to ensure that all applicable safety requirements and objectives are met.
MIL-STD-882C tasks imposed on this program are discussed in detail in section 5.

1.4 Applicable Documents

Documents identified in 1.4.1 and 1.4.2 below form an integral part of this Plan.

1.4.1 Compliance Documents.

- Contract NAS8-39225
- GP-B Systems Effectiveness Plan DR No. 802 PA-01
- EWR 127-1, Range Safety Requirements
- OSHA CFR 29
- CAL OSHA, Title 8, State of California Admin. Code, General Industry Safety Orders, Subchapter 7
- Stanford University Safety Manual
- Hazardous Materials Management Plans (HMMP)
- Chemical Hazard Communication Policy (CHCP)
- Injury and Illness Prevention Plan (IIPP)
- Acutely Hazardous Materials Plan (AHMP) and Risk Management Prevention Plans (RMPP)

1.4.2 Guidance Documents

- MIL-STD-882C, System Safety Program Requirements
- MSFC NMI 8621.1F, Mishap Reporting & Investigation

1.4.3 Reference Documents

- LMMS/P086904, Gravity Probe B, Relativity Mission, System Effectiveness Plan, (Spacecraft), Chapter 2.
- LMSC-F428533E, GP-B, Safety, Reliability, Maintainability and Product Assurance Plan, (Payload), Chapter 3.
- LMSC-F277277, Science Mission Payload Specification.

2.0 ACRONYMS AND DEFINITIONS

2.1 Acronyms

AHM - Acutely Hazardous Materials
CDR - Critical Design Review
CHP - Chemical Hygiene Plan
DR - Data Requirement or Discrepancy Report
ESD - Electro Static Discharge
EH & S - Environmental Health & Safety
FMEA - Failure Mode and Effect Analysis
FSR - Facility Safety Reviews
GOP - Ground Operations Plan
GP-B - Gravity Probe B
GSE - Ground Support Equipment
HMMP - Hazardous Materials Management Plan
IHA - Interface Hazard Analysis
IIPP - Injury and Illness Prevention Plan
LMMS - Lockheed Martin Missile Systems
MSFC - Marshall Space Flight Center
MSPSP - Missile System Pre-launch Safety Package
OHA - Operating Hazard Analysis
PDR - Preliminary Design Review
PHA - Preliminary Hazards Analysis
PHL - Preliminary Hazard List
PM - Program Manager
PPS - Product Protection Standards
QA - Quality Assurance
RMPP - Risk Management Prevention Plans
SEM - System Effectiveness Manager
SHA - System Hazard Analysis
SOW - Statement of Work
SP - Safety Plan
SSA - Software Safety Analysis
SSE - System Safety Engineer
SSHA -Subsystem Hazard Analysis
SSP - System Safety Program
SSPP - System Safety Program
SSWG - System Safety Working Group
SU - Stanford University
SV - Space Vehicle
VTL - Verification Tracking Log

2.2 Definitions

Definitions provided below have been extracted from MIL-STD-882C and modified as required to apply to GP-B Program SSPP activities.

Condition. An existing or potential state such as exposure to harm, toxicity, energy source, activity, etc.

Contractor. A private sector enterprise or the organizational element of NASA or any other Government agency engaged to provide services or products within agreed limits specified by the managing agency (MA).

Fail safe. A design feature that ensures that the system remains safe or in the event of a failure will cause the system to revert to a state which will not cause a mishap.

Hazard. A condition that is prerequisite to a mishap.

Hazard probability. The aggregate probability of occurrence of the individual events that create a specific hazard.

Hazard severity. An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

Hazardous material. Anything that due to its chemical, physical, or biological nature causes safety, public health, or environmental concerns that result in an elevated level of effort to manage.

Managing activity. The organizational element of Government assigned acquisition management responsibility for the system, or prime or associate contractors or subcontractors who impose system safety tasks on their suppliers.

Mishap. An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. Accident.

Nondevelopmental item.

a. Any item of supply that is available in the commercial marketplace;

b. Any previously developed item of supply that is in use by a department or agency of the United States, a state or local government, or a foreign government with which the United States has a mutual defense cooperation agreement;

c. Any item of supply described in definition a. or b. , above, that requires only minor modification in order to meet the requirements of the procuring agency; or

d. Any item of supply that is currently being produced that does not meet the requirements of definition a., b., or c., above, solely because of the item is not yet in use or is not yet available in the commercial marketplace.

Risk. An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability.

Risk assessment. A comprehensive evaluation of the risk and its associated impact.

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

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

Safety critical computer software components. Those computer software components and units whose errors can result in a potential hazard, or loss of predictability or control of a system.

System Safety Program Plan. A description of the planned tasks and activities to be used by the contractor to implement the required system safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

Subsystem. An element of a system that, in itself may constitute a system.

System. A composite, at any level of complexity, of personnel, procedures, materials, 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 purpose, support, or mission requirement.

System safety. The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

System safety engineer. An engineer who is qualified by training and/or experience to perform system safety engineering tasks.

System safety engineering. 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 group/working group. A formally chartered group of persons, representing organizations initiated during the system acquisition program, organized to assist the MA system

program manager in achieving the system safety objectives. Regulations of the military components define requirements, responsibilities, and memberships.

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

Systems effectiveness manager. A person responsible to program management for setting up and managing the system safety program.

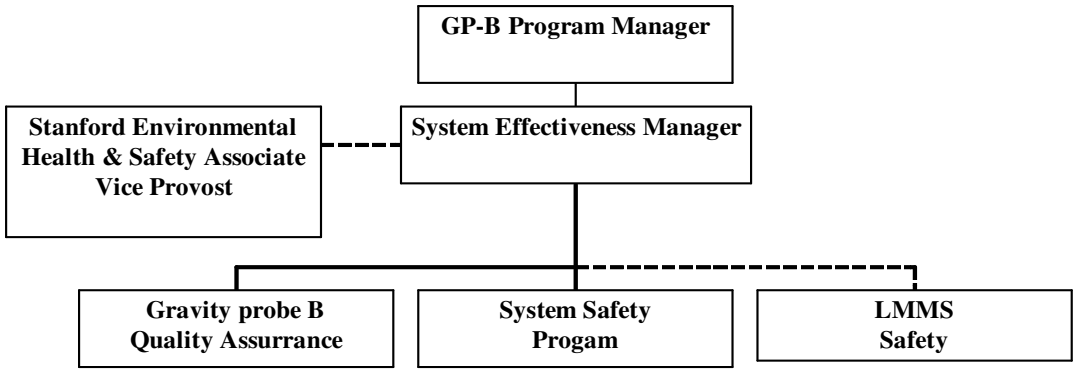
System Safety Program. The combined tasks and activities of system safety management and system safety engineering implemented by acquisition project managers.

3.0 SAFETY ORGANIZATION RESPONSIBILITIES AND AUTHORITY

3.1 Functional Organization

The safety organization consists of the Stanford Environmental Health & Safety Associate Vice Provost, GP-B Program Manager, System Effectiveness Manager (SEM).

Figure 1, Safety Organization Chart



Legend: Dashed line represent support function

Stanford Department of Environmental Health and Safety Officer (EH&S) and the System Safety Engineers (SSE). The chart at Figure 1 illustrates organizational and functional relationships and lines of communication of the system safety organization.

3.2 Responsibilities

3.2.1 Program Manager (PM)

The PM will provide the necessary support for the planning, organization, coordination, and implementation of the system safety program objectives. The PM is the authority to resolve all hazards identified to the GP-B Program. Risk acceptance authority varies according to the degree of risk involved. Risk is determined by performing hazard analyses tasks discussed in Section 4.0 & 5.0 below.

3.2.2 System Effectiveness Manager (SEM)

The SEM for the GP-B Program is responsible for the overall GP-B system safety program and is directly accountable to the Program Manager (PM). The SEM reports directly to the PM for GP-B. SSPP activities and has direct access to all design and development information and staff. The SEM serves as the point of contact for all GP-B Program system safety matters and has oversight responsibility for system safety activities of the SU SSE and the major subcontractor, Lockheed Martin Missiles & Space (LMMS).

3.2.3 System Safety Engineer (SSE)

The SSE will be responsible for establishing liaison with contractor, subcontractor and vendor system safety personnel and for carrying out procedures developed by the SEM. The SSE responsibility will not be performed by one individual for the Gravity Probe B Program. SSE tasks will be accomplished by tasking/subcontracting qualified safety organizations or personnel to ensure system safety requirements are met. (Refer to Figure 1) Some of these tasks include:

- Prepare documentation and report on required safety analyses.
- Review safe and successful designs of similar systems to aid in the definition of GP-B Program system safety requirements.
- Update hazard analyses as necessary to ensure those safety concerns resulting from engineering changes proposals (ECP) receive appropriate action.
- Identify hazards eliminated by design changes in the system or minimized by control measures.

- Conduct safety reviews of proposed operating and maintenance procedures, or changes, to ensure that applicable warnings and cautions are established.

- Document hazardous conditions and system deficiencies to assist in developing follow-on requirements for modified or new systems.

- Participate in design and program reviews and present results of hazard analyses.

- Evaluate results of failure investigations and recommend design actions or other corrective actions necessary.

- Review engineering documentation and technical publications and provide inputs and corrections as needed.

- Verify the adequacy of safety and warning devices.

- Participate as an active member of the Configuration Change Control Board.

- Participate in and support system safety working groups.

3.2.4 Occupational Safety

Good health and safety practices are a responsibility of each faculty member, staff member, and student. Line responsibility for good health and safety practice begins with the supervisor in the workplace, laboratory or classroom and proceeds upward through the levels of management.

In academic areas, supervisors include the lab directors, class instructors, principal investigators, or others having direct supervisory authority. Academic levels of management are the department chairperson or Independent Lab director, dean, the Dean of Research, and the Provost. Administrative levels of management include mid-management, directors, and vice presidents. Final responsibility for health and safety policy and programs rests with the President of the University.

3.2.4.1 Stanford University Associate Vice Provost of Environmental Health & Safety

Stanford University Associate Vice Provost of Environmental Health & Safety (also the Director of Environmental Health and Safety) will:

- Review the SSPP, as it applies to EH&S, and sign it on behalf of Stanford University.

- Provide technical services for the EH&S activities at GP-B.
- Provide technical information on Federal and State safety compliance requirements and scheduled safety inspections of laboratories, as needed.
- Recommend University-wide health and safety policies.
- Ensure overall institutional compliance with policies, statutes and regulations.
- Monitor the effectiveness of the safety programs.
- Provides central health and safety services to all areas of the University.

The Department of Environmental Health and Safety (EH&S) at Stanford University is tasked to supply all facility safety monitoring of GP-B on campus facilities, if determined necessary by EH&S technical staff. Their designated representatives are tasked to provide technical assistance to aid GP-B personnel in complying with all OSHA requirements. They will be responsible for providing technical support, information, and services in areas such as Environmental Health and Safety, Industrial Hygiene, and Industrial Safety for the duration of the program. Refer to Stanford's Safety Manual, Radiation Protection Manual, Laser Safety Manual, and Biosafety Manual for further safety information in these areas. Any violations or findings will be documented and forwarded to the SEM.

EH&S is responsible for development and implementation of Stanford's Hazardous Materials Management Plans (HMMP), Chemical Hygiene Plan (CHP), Injury and Illness Prevention Plan (IIPP), and the Acutely Hazardous Materials (AHM) & Risk Management Prevention Plans (RMPP).

3.2.4.2 Supervisor Responsibilities

All University supervisors, including faculty supervisors, are responsible for protecting the health and safety of employees and students under their supervision. This responsibility entails:

- Implementing Stanford University health and safety policies, practices, and programs.
- Ensuring that workplaces and equipment are safe and well maintained.
- Ensuring that workplaces or laboratories are in compliance with Stanford policies, Programs, and practices.

3.2.4.3 Manager Responsibilities

All University managers, academic and administrative, are responsible for ensuring that:

- Individuals under their management have the authority to implement appropriate health and safety policies, practices, and programs.
- Areas under their management have adequate funding for health and safety programs, practices, and equipment.
- Areas under their management are in compliance with Stanford University health and safety policies, practices and programs.

3.2.4.4 EH&S Responsibilities

Environmental Health and Safety (EH&S) is responsible for:

- Reviewing legislation, recommending policies, and monitoring compliance with environmental and health and safety statutes and regulations and University health and safety policies and programs.
- Providing guidance and technical assistance to supervisors and managers in the schools, departments, and other work units in identifying, evaluating, and correcting health and safety hazards.
- Developing programs for the safe use of hazardous radiological, biological, and chemical substances and lasers.
- Providing training materials, assistance, and programs in safe and healthy work Practices.
- Providing emergency services for incidents involving hazardous materials.
- Providing fire prevention and investigation services.
- 0perating hazardous waste disposal services.
- Review all procedures that involve all potentially hazardous activities.
- Provide oversight during the implementation of potentially hazardous procedures.
- Manage regulatory compliance programs for chemical storage and use.

- Perform random surveys of laboratory Operations.

- Schedule county health inspections and accompany inspectors. Assists labs and shops in following through on complaints and citations.

- Controls chemical hazards information management system [material safety data sheets (MSDS) and life safety boxes].

- Maintain Stanford's Chemical Safety Database and EH&S' master set of material safety data sheets.

- Provide annual safety training to Stanford personnel.

While EH&S is responsible for developing and recommending policies, policy approval rests with other University bodies, e.g. Faculty Senate, Dean's Cabinet, Operations Council, University Health and Safety Committee, Committee on Research, Administrative Panels, depending on the content of the proposed policies.

3.2.4.5 Employee and Student Responsibilities

Employees and students are responsible for:

- Keeping themselves informed of conditions affecting their health and safety.

- Participating in training programs provided by their supervisors and instructors.

- Adhering to healthy and safe practices in their workplace, classroom, laboratory, and student campus residences.

- Advising their supervisors or instructors of serious hazards in the workplace, classroom, or laboratory.

3.3 Program Interfaces

Interface between other functional disciplines of the GP-B Program and the SSE is a must. The SSE will review and/or analyze inputs received from other functional disciplines, and provide outputs as required by this plan or as approved by the SEM. An example of typical program interfaces is illustrated in Figure 3.

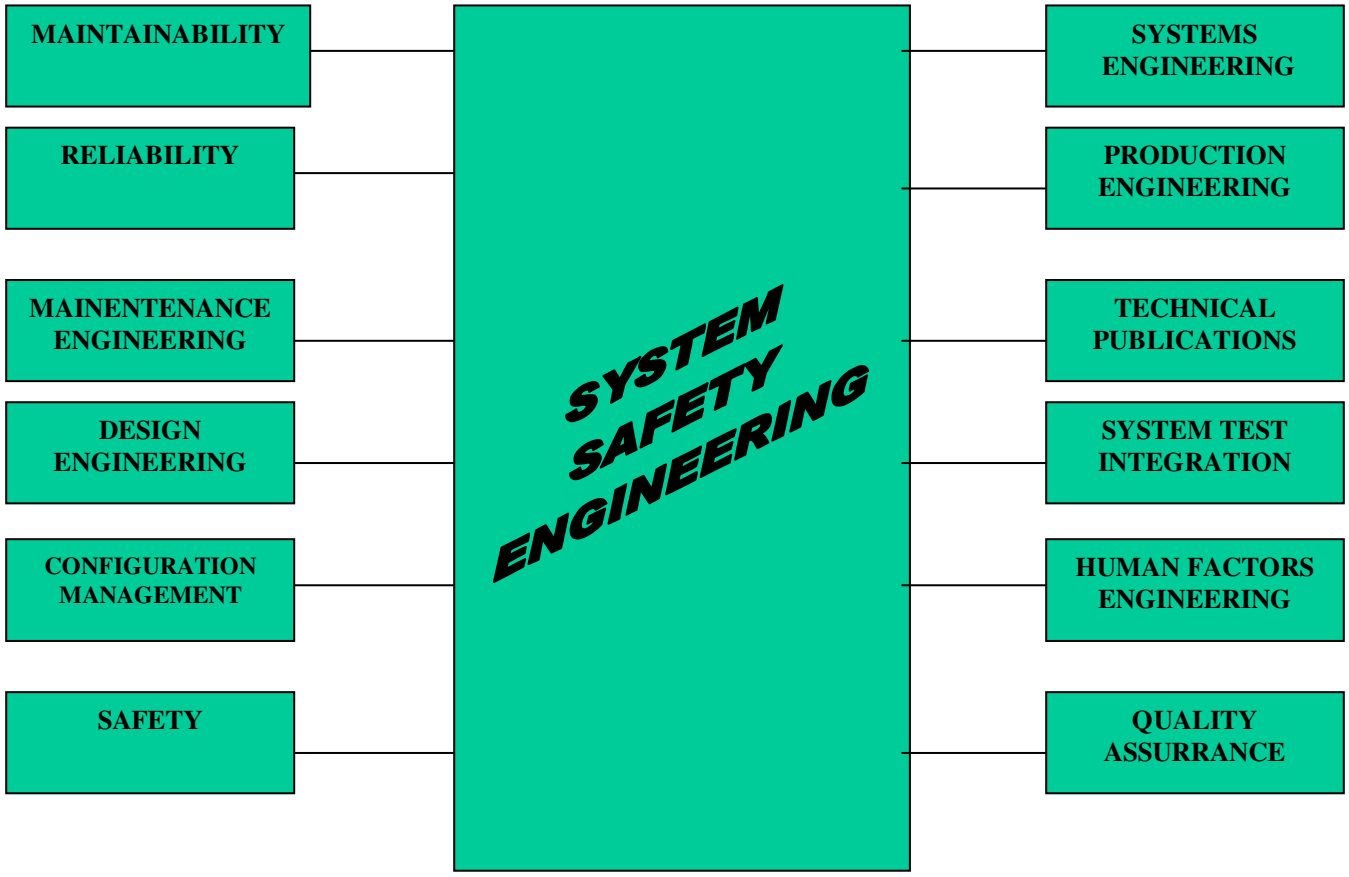


Figure 3. PROGRAM

3.4 Authority

The SEM has been delegated the necessary authority by the GP-B PM to act upon or perform the following:

- Make immediate corrective actions upon receiving notification of critical/catastrophic hazards.

- Notified upon occurrence of mishaps or malfunctions and respond as necessary.
- Review and make recommendations regarding safety requirement waivers and program deviations.
- Impose design requirements and special safety test requirements.
- Review and monitor contractor, subcontractor and vendor system safety activities.
- Analyze system design and monitor program test activities.
- Call design and special safety reviews, and participate in trade-off studies that could affect the safety of the system.
- Impose procedural control requirements in technical manuals and impose safety training requirements.
- Maintain a system safety engineering capability consistent with requirements of the program.

3.5 Contractor, Subcontractor and Vendor Responsibilities

Contractors, subcontractors and vendors to the GP-B Program, other than those supplying non-developmental items, will be required to develop a system safety program which meets the intent of MIL-STD-882C, Task 101. Contractors, subcontractors and/or vendors supplying nondevelopmental items originally designed to MIL-STD-882, current or previous versions, will be required to provide the system safety documentation generated during the design and manufacture of that equipment. For equipment not designed to the requirements of MIL-STD-882, the contractor, subcontractor and/or vendor will be required to provide product safety data indicating the applicable general industry and OSHA standards to which the equipment was designed and manufactured. In all cases, these documentation and data must show compliance with applicable safety requirements.

3.6 System Safety Working Group

A System Safety Working Group (SSWG) will be formed to advise and assist the GP-B PM in developing, coordinating and implementing safety policies, procedures, and actions affecting the GP-B Program. As an advisory and coordinating group, the SSWG will not have tasking or approval authority. Tasking will be through normal organizational channels. The GP-B PM, or his delegate, will serve as chairperson of the SSWG which will be comprised of members primarily from various program safety offices. A primary and alternate member will be requested from each organization involved in the GP-B Program. Other interested organizations will be invited to participate in the SSWG as associate members. The GP B will hold quarterly technical

interchange meetings (TIM) that include members of the SSWG. The status of the SSP will be presented at the TIMs and any relevant issues discussed.

Organizations providing SSWG participating members are:

- NASA Marshall Space Flight Center GP-B Program Office
- Stanford University
- Lockheed Martin Missiles & Space

Organizations which may provide associate members are:

- 30th Space Wing, Vandenberg Air Force Base (VAFB)
- Boeing Aerospace (Delta II Project Office)

3.7 Staffing

The SEM will ensure staffing for the GP-B Program is consistent with the technical requirements of the program. Desired qualifications for a system safety engineer includes an appropriate Bachelor of Science degree and at least four years relevant experience in system safety, preferably in the aerospace industry. A working knowledge of quality and reliability engineering is desired. A certification as a safety professional is preferred.

4.0 SYSTEM SAFETY CRITERIA

4.1 Design Criteria

System safety criteria, based upon the application of EWR 127-1, shall be developed and used by System Safety Engineering to assess design compliance. The results of this assessment are presented by the GP-B System Safety Engineer or his designee at the safety reviews. All subsystem designers are required to demonstrate compliance of their system with safety requirements. Action items resulting from any technical review having a safety impact will be jointly assigned to the responsible engineer and the System Safety Engineer. The System Safety Engineer will be responsible for:

a. Maintaining an independent safety action item log listing all program safety related action items, responsible engineer and closure status.

b. Ensuring the adequacy and implementation of the response.

c. Signing the response as an indication of acceptance (verification).

Open items will be reported to GP-B Program Management and will be carried as part of a Hazard Analysis Report where appropriate. Verification data for each identified hazard control will be incorporated into the MSPSP - Missile System Prelaunch Safety Package, for flight systems and GSE, and the GOP - Ground Operations Plan, for operations at the Western Range.

4.2 System Safety Precedence

Actions for satisfying safety requirements and criteria, as well as eliminating identified hazards or reducing the associated risk (in order of precedence) shall be implemented as follows:

a. Design for Minimum Hazard. 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, and shields.

c. Protective Systems. Where accident risk exists and cannot be totally eliminated, the employment of systems to prevent injury to personnel, property, or the equipment is acceptable risk reduction. Such systems include, for example, fire suppression, radiation shields, and blast shields.

d. Warning Devices. Where it is not possible to preclude the existence or occurrence of an identifiable hazard, devices will be employed in the Ground Support Equipment (GSE) 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 preset limits are exceeded. Examples of such devices are indicator-type fuses, high- or low-temperature monitors, high- or low-pressure monitors, and shock recorders.

e. Special Procedures. Special procedures will be developed whenever it is not possible to reduce the magnitude or probability of an existent or potential hazard by means of the above efforts and devices.

4.3 Hazard-Level Categories

4.3.1 Hazard-Level Definitions

For Hazard Analysis and other tasks described in this Plan, Hazard Severity Categories will be per Table 1 is based on Table 1 in MIL-STD-882C, paragraph 4.5.1.

Table 4. 1. Hazard Severity Categories

Description	**Category**	**Definition**
Catastrophic	I	Death, system loss, or severe environmental damage.
Critical	II	Severe injury, severe occupational illness, major system or environmental damage.
Marginal	III	Minor injury, minor occupational illness, or minor system or environmental damage.
Negligible	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Hazard Probability Levels will be per Table 2, which is based on Table 2 in MIL-STD-882C, paragraph 4.5.2. The “Fleet or Inventory” column was found not applicable for GP-B Program.

Table 4.2. Hazard Probability Levels

Description	Level	Specific Individual Item.
Frequent	A	Likely to occur frequently.
Probable	B	Will occur several times in the life of an item.
Occasional	C	Likely to occur some times in the life of an item.
Remote	D	Unlikely but possible to occur in the life of an item.
Improbable	E	So unlikely, it can be assumed occurrence may not be experience.

4.4 Risk Assessment

Decisions regarding resolution of identified hazards will be based on assessment of the risk involved. To aid in the achievement of the objectives of system safety, hazards shall be characterized as to hazard severity categories and hazard probability levels, when possible. Based on a combination of these hazard severity categories and hazard probability (frequency) levels, hazards will be assigned a risk assessment code (RAC). RAC 1 will reflect the most hazardous combination and RAC 4 the least. RACs will form the basis for establishing priorities and resource expenditures for controlling identified hazards.

Table 4.3. Risk Assessment Codes (RAC'S)

CONSEQUENCE CATEGORY				
FREQUENCY OF OCCURRANCE	**(I) CATASTROPHIC**	**(II) CRITICAL**	**(III) MARGINAL**	
(A) FREQUENT	**1**	**1**	**1**	**3**
(B) PROBABLE	**1**	**1**	**2**	**3**
(C) OCCASIONAL	**1**	**2**	**3**	
(D) REMOTE	**2**	**2**	**3**	
(E) IMPROBABLE	**3**	**3**	**3**	

HAZARD RISK INDEX	RISK ASSESSMENT CODE	ACTION REQUIRED
IA, IB, IC,IIA, IIB,IIIA	1	UNACCEPTABLE-IMMEDIATE COORECTIVE ACTION
		NASA DECISION
ID, IIC, IID, IIIB	2	UNDESIRABLE-REDUCED PRIORITY,
		C/A INCLUDING MSPC CONCURRENCE REQUIRED
IE, IIE, IIIC, IIID,IIE, IVA,IVB	3	ACCEPTABLE-LOW PRIORITY FOR C/A (MAY NOT WARRANT ACTION)
		SEM DECISION
IVC, IVD, IVE	4	ACCEPTABLE - NO C/A REQUIRED

4.5 Risk Acceptance

Once an assessment of a particular risk is completed, the PM and SEM may evaluate the possibility of accepting the identified hazard as a program risk. There may be circumstances when the GP B program may decide to accept a particular risk. Risk acceptance authority will depend on the RAC level of the identified hazard. Those hazards assigned a RAC 3 will require a Discrepancy Report (DR) be generated by the SEM and dispositioned, explaining the rationale for accepting the risk. Although unlikely, if the program decides to accept the risk of a hazard with an RAC of 1 or 2, a waiver or deviation will be generated. The waiver/deviation will need approval from the SEM, GP B PM, MSFC and NASA depending on the RAC category.

5.0 SYSTEM SAFETY PROGRAM TASKS

There are two task types referred to in MIL-STD-0882C. These are system safety engineering tasks and system safety management tasks. They are described in more detail in paragraphs 5.2 and 5.3. Task selection is an important function of developing an acceptable and cost-effective SSPP. The elements of a SSPP must be selected to meet GP-B Program safety needs. These needs are identified by higher authority through directives, regulations, instructions, or in this case, the SP. Identifying these needs must be accomplished prior to the applicable acquisition or operational phase so that tasks and requirements are commensurate with the needs of the SSPP. Prioritizing or establishing a baseline group from all tasks contained in MIL-STD-882C cannot be accomplished unless variables like system complexity, program phase, availability of funds, schedule, etc. are known. For the GP-B Program, some of this information may be available as a result of planned and specific steps of incremental verification. This incremental verification concept was the foundation of the predecessor contract (NAS8-36125) initiated in 1985.

Figure 5-1 illustrates SSPP activities associated with Interim Response Actions, such as those that may be encountered in the GP-B Program life-cycle.

5.1 System Safety Program Management Tasks

As the term implies, system safety management tasks are tools for the SEM to use while managing the SSPP. Task 101, System Safety Program, is a required task when MIL-STD-882C is imposed. All other tasks require task 101 as a prerequisite. Other management tasks are selected based on a number of variables, such as program size and anticipated risk. For the GP-B Program, the following tasks will be implemented:

Task 101 - System Safety Program
Task 102 - System Safety Program Plan (Safety Plan)
Task 104 - System Safety Program Reviews/Audits
Task 105 - System Safety Group/System Safety Working Group Support
Task 106 - Hazard Tracking and Risk Resolution

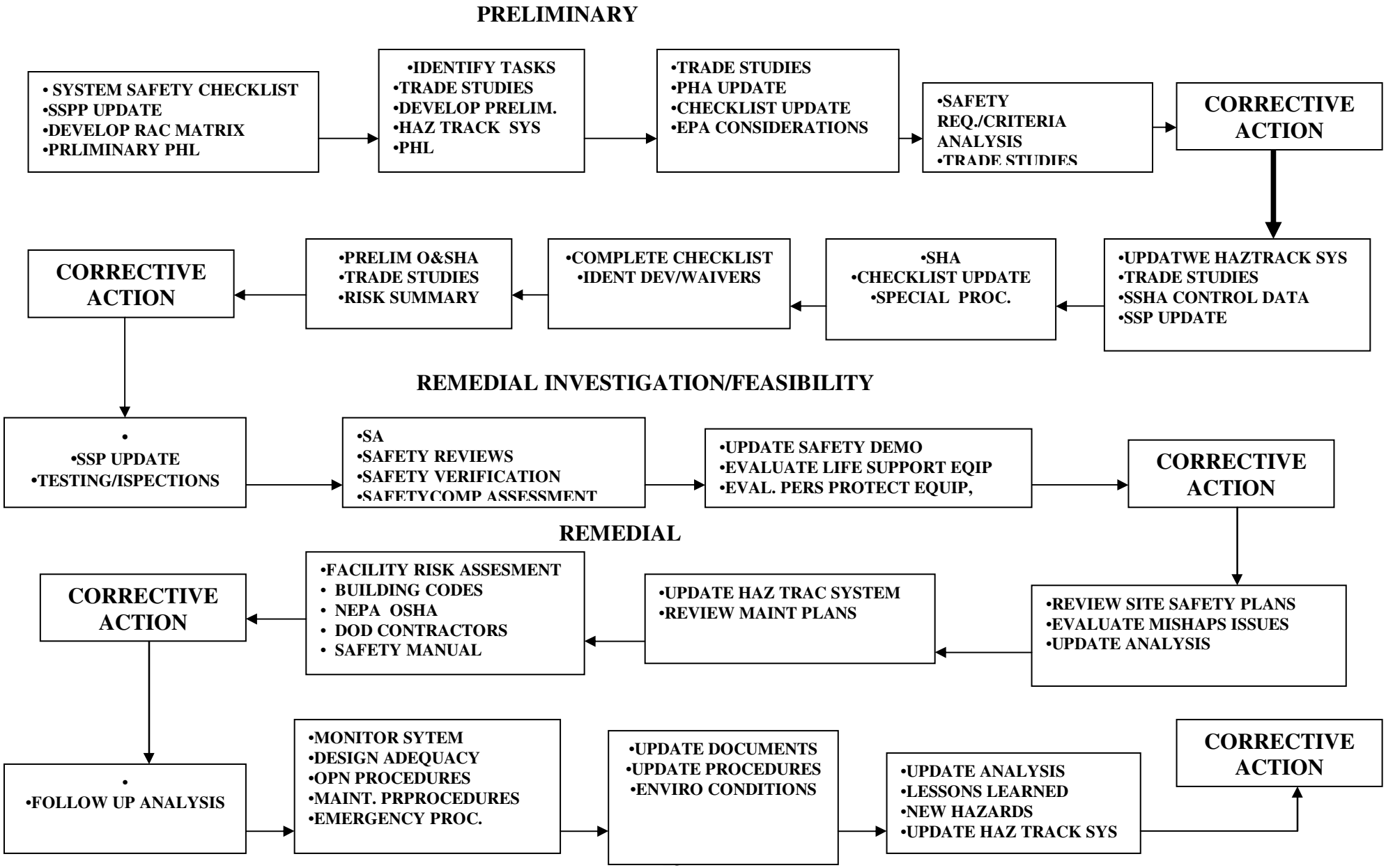


FIGURE 5.1. SYSTEM SAFETY TASK FLOW DIAGRAM

5.1.1 System Safety Program

This task establishes the foundation for a SSP to meet the tailored requirements of MIL-STD-882C Section 4, General Requirements, and all other tasks/requirements as designated. The SSPP task facilitates development of a planned approach for task accomplishment, establishment of a system safety organization and interfaces between other disciplines, and definition of SSPP milestones.

5.1.2 System Safety Program Plan (Safety Plan)

The SP task develops a SSPP that details tasks and activities of system safety management and engineering required to identify, evaluate, and eliminate/control hazards, or reduce the associated risk to an acceptable level. The SP provides a basis of understanding between program elements, contractors, and subsystem SSPPs concerning how the top-level SSPP will be accomplished to meet program requirements.

5.l.3 System Safety Program Reviews/Audits

This task establishes a requirement for new major and minor subcontractors to perform and document SSPP reviews/audits or support reviews/audits performed by the GP-B Program SEM. Results of reviews and audits will be provided to the Level II MSFC Safety and Mission Assurance (S&MA) Manager so that they may be used to supplement the Level II program review/audit requirements.

5.1.4 System Safety Group/System Safety Working Group Support

This task requires GP-B Program prime and major contractors to support the GP-B System Safety Working Group (SSWG) as defined by the GP-B Program PM and SEM.

5.1.5 Hazard Tracking and Risk Resolution

Establishes a single, closed-loop hazard tracking system to track hazards to flight hardware and their controls, thus providing an audit trail of hazard resolutions. It is anticipated that the hazard tracking system for the GP-P program will be a computer-support database.

5.2 System Safety Program Engineering Tasks

System safety engineering tasks involve system hazard analyses, safety assessments, tests and evaluations, and safety verifications. Hazard analyses are performed to identify hazards or hazardous conditions for flight hardware and determine how to eliminate the hazard or find effective hazard controls. The level of effort required for the analysis task will vary somewhat according to the complexity of the system or subsystem being analyzed. Table 5-1 presents a hazard identification checklist that will assist in identifying hazards for performing GP-B Program hazard analyses and developing a preliminary hazard list (PHL). Safety assessments are performed to document a comprehensive evaluation of a mishap risk being assumed prior to the test or operation of a system, prior to the next contract phase, or at contract completion. Tests and evaluations ensure safety is considered and safety responsibility assigned in test and evaluation, to provide existing analysis reports and other safety data and respond to all safety requirements necessary for system testing. Safety verification defines and performs tests and demonstrations or uses other verification methods on safety critical hardware, software, and procedures to verify compliance with safety requirements. For the GP-B Program, the following tasks will be implemented:

Task 202 - Preliminary Hazard Analysis (PHA)
Task 203 - Subsystem Hazard Analysis (SSHA)
Task 204 - System Hazard Analysis (SHA)
Task 206 - Operating and Support Hazard Analysis (O&SHA)
Task 401 - Safety Verification

Table 5-1. HAZARDS GROUPS FOR PRELIMINARY HAZARDS LIST

Hazard Group	Example Hazards
	ENERGY SOURCE
Corrosive Chemical	Material degradation, galvanic actions
Electrical	Commercial power, batteries, received radio frequency, moving insulators, lightning induced static, resistive heating effects on flight hardware
Kinetic Mechanical	Moving equipment and objects, personnel working surfaces risks to flight hardware

Potential Mechanical	Overhead objects, high work, lifting devices risks on flight hardware
Pressure	Hydraulics, vacuum risks on flight hardware
Noise	Distraction, communication disruption effects on flight hardware
Radiation	Laser, ionizing, optical effect on flight hardware
Stored Chemical	Fuels, explosives, hypergolic materials effects on flight hardware
Temperature Differential	Heat source, cryogenics, embrittlement effects on flight hardware
TOXIC/HARMFUL	
Asphyxiants	Halon, nitrogen, confined entry gases effects on flight hardware
CSM	Chemical Surety Materiel, GB, VX, Mustard, BZ effects on flight hardware
Temperature Extremes	Cold/wet (hypothermia), hot/humid (heat gas, liquid, or solid; acute/chronic effects on flight hardware
Other	Flight hardware hazards not otherwise specified

5.2.1 Preliminary Hazard Analysis (PHA)

Using the PHL as a basis, the PHA is conducted by adding the actions recommended to control the identified hazards to an acceptable level and specifying the controlled RAC and any related standards or regulations with which compliance is required. The purpose of the PHA is not to actually establish control for every identified hazard, but to describe completely the magnitude of the hazards to flight hardware and efforts required to control them.

The results of the PHA may be used to select subsystems or components for more detailed analytical processes [e.g., Failure Modes and Effects Analysis (FMEA) or Fault Tree Analysis

(FTA)], to establish design and operating criteria to enhance safety, and to initiate the hazard tracking process.

5.2.2 Subsystem Hazard Analysis

The Subsystem Hazard Analysis is used to identify hazards associated with the design of subsystems, including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem. The PHA and hazard tracking log formats are normally used.

5.2.3 System Hazard Analysis

An SHA is conducted to assemble the various subsystem or component PHAs and assess overall system hazards. Hazards identified in PHAs are not re-introduced, but rather a different emphasis is used to identify new hazards. This emphasis is on identifying hazards resulting from interfaces, failure of safety devices, common cause and simultaneous failures, non-failure degradation, design changes, safety criteria non-compliance, and human error. The PHA and hazard tracking log formats are normally used, but FMEA and FTA techniques and formats are also appropriate.

5.2.4 Operating and Support Hazard Analysis

The O&SHA is performed on selected subsystems and components to identify and evaluate the hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of the subsystem or component. The emphasis is on personnel activities effects on flight hardware (both operating and maintenance), draft SOPs and operating manuals, human factors, and people or procedure induced hazards. The PHA and hazard tracking log formats are normally used, but FMEA and FTA techniques and formats may also be appropriate.

5.2.5 Safety Verification

Safety Verification is used to define and perform tests and demonstrations or use other verification methods on safety critical hardware, software, and procedures to verify compliance with safety requirements. Safety verification is useful where hazards are identified during the design effort and it cannot be determined by analysis or inspection whether the action taken will adequately reduce the risks.

5.2.6 Deliverable Safety Documents

GP-B will submit a Missile Systems Prelaunch Safety Plan (MSPSP) and a Ground Operations Plan (GOP) in accordance with the requirements in EWR 127-1.

The MSPSP provides a detailed description of hazardous and safety critical ground support and flight hardware equipment, systems, and materials their interfaces. A draft of the MSPSP will be provided at CDR, with a final submission which satisfies all Range Safety concerns provided at least 45 days prior to shipment of the hardware to the Range.

The GOP provides a detailed description of hazardous and safety critical operations associated with the space vehicle and its' associated ground support equipment. A draft of the GOP will be provided no later than one year prior to the projected date hardware will arrive at the Range, with a final submission which satisfies all Range Safety concerns provided at least 45 days prior to shipment of the hardware to the Range.

The MSPSP and GOP are constantly evolving documents. Official interim submittals of the MSPSP and GOP will not be made, however, sections of the MSPSP and GOP will be reviewed as appropriate during the quarterly Safety Working Group Meetings in order to assure that Range Safety's concerns are being appropriately covered.

6.0 USE OF SYSTEM SAFETY DATA

Safety data from similar systems developed for other programs, and lessons learned from other programs, will be used as much as possible in performing system safety tasks for the GP-B Program. In addition to lessons learned, other sources of safety data are current and historic mishap data and identified hazards maintained in the tracking system.

Documentation and files for the GP-B Program will consist of lessons learned from other programs/systems, task-driven studies, hazard identification checklists, analysis reports, hazard analysis worksheets and control logs, design reviews, operating logs, failure reports, and minutes of technical interchange and SSWG meetings

7.0 TRAINING

Specific training requirements for SU and subcontractor personnel will differ in terms of complexity and magnitude because of the wide variation of activities between subsystems. DID DI-SAFT-80100A (found in Appendix D, MIL-STD-882C) requires that each SP identify "techniques and procedures to be used to ensure that the objectives and requirements of the system safety program are met in the safety training for engineers, technicians, programmers, and testing, operating, and maintenance personnel." The SEM must evaluate program requirements to determine applicable training needed.

8.0 MISHAP REPORTING AND INVESTIGATING

The reason for developing a mishap reporting and investigation process for the GP-B Program is to ensure mishaps, or near misses, which may have resulted from design, procedural, or other correctable programmatic discrepancies, are identified and resolved in a timely manner. This programmatic mishap reporting and investigation process serves to supplement any mishap reporting processes required by Federal, State or local laws or those imposed by NASA Management Instruction (NMI) 8621.1F, Mishap Reporting and Investigating.

New hazards or hazardous conditions identified through the mishap reporting and investigation process will be analyzed to determine the appropriate corrective action, assigned a hazard identification number, and tracked to closure via the hazard tracking system.

9.0 SCHEDULE

The following table includes the schedule of safety compliance data packages:

Scheduled Safety Compliance Data Packages	Due Date
Draft MSPSP delivery	Delivered at Spacecraft CDR 2
Final MSPSP delivery from LMMS to Stanford	3 months prior to Space Vehicle delivery to VAFB.
Draft GOP/Launch Site Safety Plan delivery to Stanford	12 months prior to Space Vehicle delivery to VAFB.
Final GOP/Launch Site Safety Plan delivery to Stanford	3 months prior to Space Vehicle delivery to VAFB.