GLAST LAT PROCEDURE, GUIDELINE	Document # **LAT-MD-00078-01**	Date Effective 3/1/01
	Author(s) Frank O'Neill	Supersedes
	Subsystem/Office Performance and Safety Assurance Group	
Document Title **GLAST LAT System Safety Program Plan**		

CHANGE HISTORY LOG

Revision	Effective Date	Description of Changes

Gamma-ray Large Area Space Telescope

(GLAST)

Large Area Telescope (LAT)

System Safety Program Plan

TABLE OF CONTENTS

ACRONYM LIST

ACD	Anticoincidence Detector
CAL	Imaging Calorimeter
CDR	Critical Design Review
DAQ	Data Acquisition System
EPO	Education and Public Outreach
EWR	Eastern and Western Range
GLAST	Gamma-Ray Large Area Space Telescope
GOP	Ground Operations Plan
IOC	Instrument Operations Center
IPO	Instrument Project Office
LAT	Large Area Telescope
MSPSP	Missile System Prelaunch Safety Package
NRL	Naval Research Laboratory
O&SHA	Operating and Support Hazard Analysis
PAIP	Performance Assurance Implementation Plan
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
SAR	Safety Assessment Report
SAS	Science Analysis Software
SLAC	Stanford Linear Accelerator Center
SSE	System Safety Engineer
SSP	System Safety Program
SSPP	System Safety Program Plan
SU	Stanford University
TKR	Tracker
UCSC	University of California at Santa Cruz

1 INTRODUCTION

This System Safety Program Plan (SSPP) is developed in accordance with EWR 127-1, Appendix 1B, for the Gamma-Ray Large Area Space Telescope (GLAST) Project. The GLAST LAT (Large Area Telescope) is a proposed instrument for high-energy, gamma-ray astronomy with an anticipated launch in 2005. It will be thirty times more sensitive than previous-generation, high energy, gamma-ray instruments, and will cover an energy range that is an order of magnitude larger. The nations collaborating in the GLAST LAT mission are USA, France, Japan, and Italy. The GLAST LAT mission is part of NASA's Office of Space and Science Strategic Plan.

1.1 Purpose

This GLAST LAT SSPP describes the tasks and activities of the GLAST LAT System Safety Program (SSP), which are required to identify the hazards of the GLAST LAT and to impose design requirements and management controls to prevent mishaps. This SSPP also states the goals and requirements of the System Safety effort and establishes the framework within which these goals can be satisfied and the requirements most efficiently and effectively fulfilled.

1.2 Scope and Objectives

The GLAST LAT SSP will cover all phases of the program including: design, development, fabrication, handling, transportation, storage, test, assembly and operation. The objective of the GLAST LAT SSPP is to define a systematic approach that insures the following.

- Safety consistent with operation, schedule and budget is optimized in the design, construction, and operation of the GLAST LAT.
- Hazards associated with the GLAST LAT system are identified and evaluated for all phases of the program.
- The risk associated with all identified GLAST LAT hazards is controlled to acceptable levels.
- New hazards are not introduced into the system through design changes.
- Requirements for retrofit actions necessary to eliminate or control hazards are minimized.

The policy of management is to design for minimum risk.

1.3 Reference Documents

EWR 127-1, Eastern and Western Range Safety Requirements

GLAST LAT Mission Assurance Requirements

GLAST Large Area Telescope Flight Investigation

KHB 1710.2D, Kennedy Space Center Safety Practices Handbook

NPG 8715.3, NASA Safety Manual

NSS/GO-1740.9B, NASA Safety Standard for Lifting Devices and Equipment

29 CFR 1910, Occupational Safety and Health Standards, Department of Labor

SLAC-1-720-70100-100, SLAC Environment, Safety, and Health Manual

2 SYSTEM SAFETY PROGRAM MANAGEMENT

This section describes the System Safety organizational relationships and responsibilities within the GLAST LAT Project. Figure 2-1 below shows the GLAST LAT Organization Chart. The LAT team consists of members from several geographically diverse organizations and is managed by the LAT Instrument Project Office (IPO) at Stanford Linear Accelerator Center (SLAC).

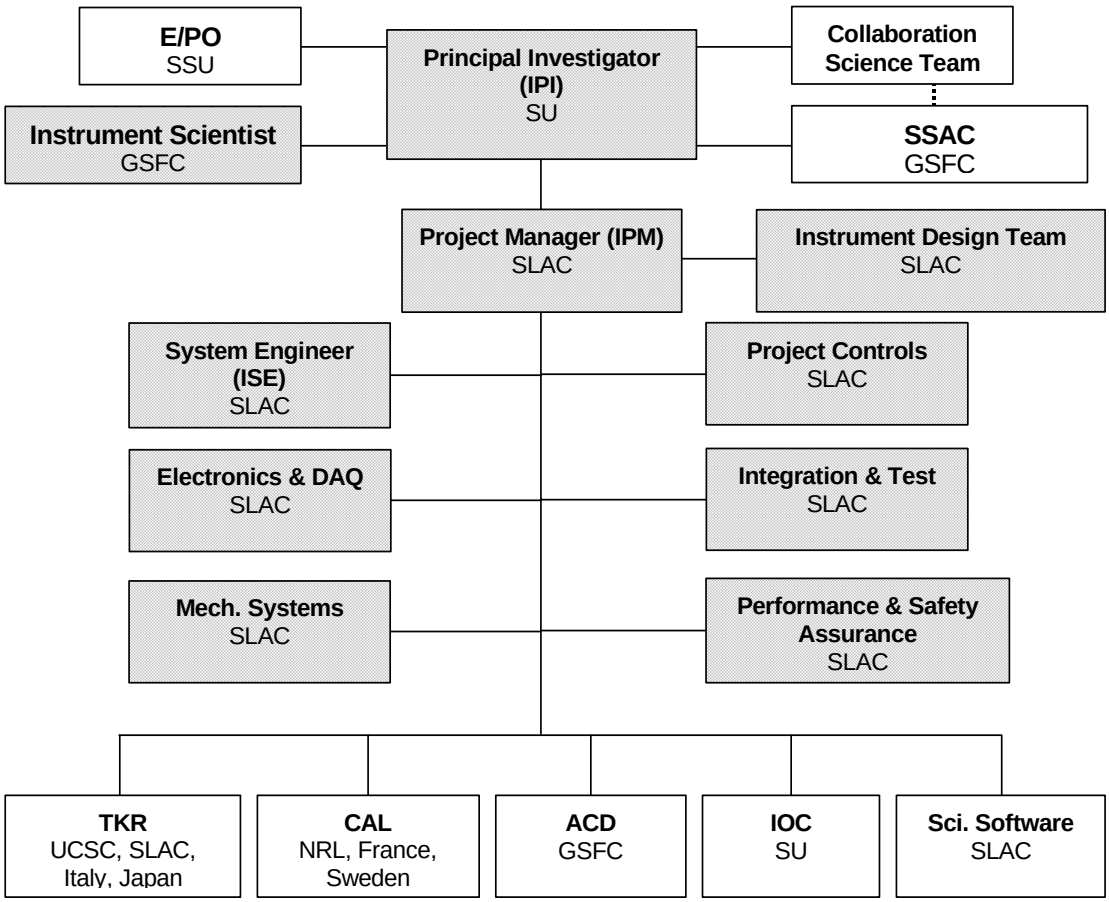


Figure 2-1 GLAST LAT Organization Chart

2.1 System Safety Program Organization, Management and Responsibilities

The GLAST LAT Project Manager has assigned a System Safety Engineer (SSE) to establish and implement the GLAST LAT SSP. The GLAST LAT SSE is organizationally located in the Performance and Safety Assurance Group, the SSE has direct access to the Project Manager to report safety issues and make recommendations to resolve them. In addition the GLAST LAT SSE reports directly to the Associate Director of the Research Division at SLAC and therefor is able to bring safety issues directly to the attention of top management of SLAC if necessary.

2.1.1 GLAST LAT Project Manager

The GLAST LAT Project Manager has the overall responsibility for ensuring that System Safety is incorporated into the GLAST LAT Project. The GLAST LAT Project Manager will implement the GLAST LAT safety policy and objectives by:

- Ensuring the SSP is established and integrated throughout the GLAST LAT Program.
- Ensuring that risk is identified and eliminated or controlled within established program risk acceptability parameters.
- Ensuring that GLAST LAT operations are performed in accordance with: applicable EWR 127-1 Range Safety Requirements, and applicable Federal, State, and Local safety regulations.
- Reviewing and approving safety analysis and documents submitted to NASA.

2.1.2 GLAST LAT System Safety Engineer

The GLAST LAT SSE is the focal point for all safety activities involved in implementing the GLAST LAT SSP. The SSE will influence the design when necessary in the interest of safety. This requires the SSE to be actively involved in many if not all aspects of the project. The SSE is responsible for:

- Participating in design reviews.
- Preparing the SSP deliverable documents.
- Support the program level interface with Range Safety.
- Developing and establishing safety design criteria and safety design requirements as needed.
- Reviewing and approving selected drawings, specifications, and procedures.
- Participating in hazardous testing and system safety testing.
- Evaluating design changes for their impact on safety.
- Participate in project activities associated with compliance to NPG 8715.3.

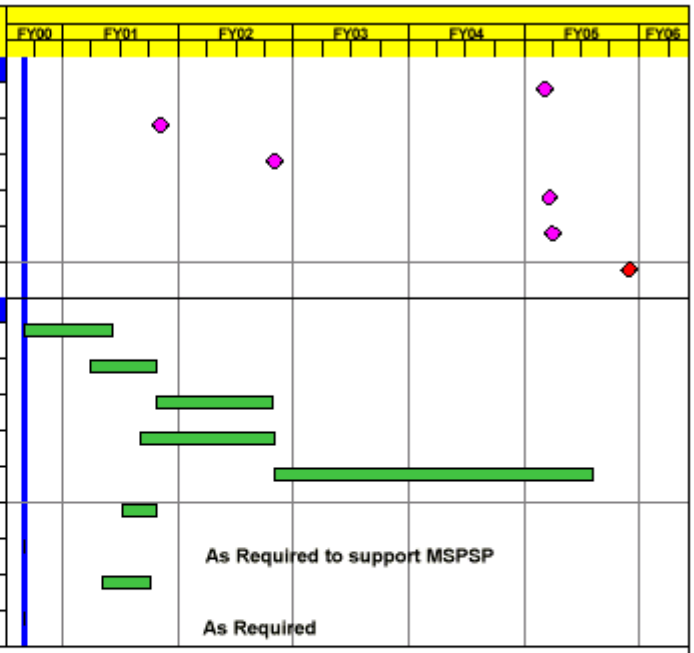
2.1.3 GLAST LAT Team Members

Each subsystem manager or designee will be responsible for integrating safety into their system and supporting the SSP as required. The LAT Subsystems include the Tracker (TRK), Calorimeter (CAL), Anticoincidence Detector (ACD), Data Acquisition System (DAQ), and Science Analysis Software (SAS). Identified members of these subsystems will directly support the SSP activities. Team members will seek technical assistance from the SSE for resolution of safety problem involving the GLAST LAT.

3 SAFETY PROJECT MILESTONES

The tasks identified below are the System Safety Deliverables for the GLAST LAT program.

Activity Description	Early Start	Early Finish	CDRL
PROJECT MILESTONES			
Pre-Ship Review	08DEC04		
Instrument PDR	06AUG01*		
Instrument CDR	05AUG02*		
Ship Instrument	22DEC04*		
Ready for Integration		28DEC04	
Launch		01SEP05*	
SYSTEM SAFETY PLAN			
System Safety Program Plan	01JUN00*	07MAR01	1
Preliminary Hazard Analysis	01JAN01	27JUL01*	2
Update PHA	30JUL01	26JUL02	2
Operating & Support Hazard Analysis	07JUN01	31JUL02*	3
Update Operating & Support Hazardous Analysis	05AUG02	06MAY05*	3
Hazard Control Verification Log	09APR01	27JUL01*	4
Safety Assessment Report	01JUN00	01JUN00	5
Ground Operations Plan Inputs	01FEB01*	04JUL01	6
Safety Noncompliance Reports	01JUN00	01JUN00	7



Sheet 1 of 1

Figure 3-1 GLAST LAT System Safety Deliverables

4 SYSTEM SAFETY METHODOLOGY

The hazard resolution method for the GLAST LAT instrument consists of the series of analytic steps depicted in Figure 4-1 and are also summarized below:

- Define the physical and functional characteristics of the proposed spacecraft by employing the information available (design documents, operating procedures, etc.), and relating the interaction between people, procedures, equipment, and the environment.

- Identify hazards related to all aspects of the GLAST LAT project and determine their causes.

- Assess the hazards to determine severity and probability, and to recommend means for their elimination or control.

- Implement corrective measures to eliminate or control the individual hazards, or accept the corresponding risks.

- Conduct follow-up analyses to determine the effectiveness of preventive measures, address new or unexpected hazards, and issue additional recommendations if necessary.

DEFINE THE SYSTEM

Define the physical and functional characteristics and understand and evaluate the people, procedures, facilities, equipment, and environment

IDENTIFY HAZARDS

Identify hazards and undesired events and determine the causes of hazards

ASSESS HAZARDS

Determine Severity
Determine Probability
Decide to accept risk or eliminate/control

RESOLVE HAZARDS

Assume risk or
Implement corrective action
- Eliminate
- Control

FOLLOW-UP

Monitor for effectiveness
Monitor for effectiveness
Monitor for unexpected hazards

Figure 4-1 Hazard Resolution Process

4.1 Hazard Assessment

The hazard assessment process is a principal factor in the understanding and management of technical risk. Hazards are identified and resultant risks are assessed by considering probability of occurrence and severity of consequence. Risk will be assessed qualitatively. System Safety is an integral part of the overall program risk management decision process.

4.1.1 Hazard Severity Categories

Severity is an assessment of the worst potential consequence, defined by degree of injury or property damage, which could occur. There are four categories of hazard severity: Class I, Catastrophic; Class II, Critical; Class III, Marginal; and Class IV, Negligible. Figure 4-2 depicts these categories and provides a general description of the characteristics that define the worst-case potential injury or system damage if the identified hazard were to result in an accident. These categories are derived from MIL-STD-882D, Standard Practices for System Safety.

4.1.2 Hazard Probability Categories

Probability is the likelihood that an identified hazard will result in a mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population. There are five levels of probability: Level A, Frequent; Level B, Probable; Level C, Occasional; Level D, Remote; and Level E, Improbable. Figure 4-3 depicts these levels and provides a general definition for each probability levels. These levels are derived from MIL-STD-882D, Standard Practices for System Safety.

Hazard Severity

CLASS	DESCRIPTION	POTENTIAL CONSEQUENCES
I	CATASTROPHIC	A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission
II	CRITICAL	A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware.
III	MARGINAL	A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware.
IV	NEGLIGIBLE	A condition that could cause the need for minor first aid treatment though would not adversely affect personal safety or health. A condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear.

Figure 4-2 Hazard Severity Classification

Hazard Probability

LEVEL	FREQUENCY OF OCCURRENCE	DEFINITION
A	Frequent	Likely to occur frequently. ($X > 10^{-1}$)
B	Probable	Will occur several times in the life of an item. ($10^{-1} \geq X > 10^{-2}$)
C	Occasional	Likely to occur some time in the life of an item. ($10^{-2} \geq X\ 10^{-3}$)
D	Remote	Unlikely, but possible to occur in the life of an item. ($10^{-3} \geq X > 10^{-6}$)
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced.

Figure 4-3 Hazard Probability Levels

4.1.3 Mishap Risk Assessment

The Risk Assessment Value is a numerical expression of comparative risk determined by an evaluation of both the potential severity of a mishap and the probability of its occurrence. The Risk Assessment Value is assigned a number from 1 to 20 from the Mishap Risk Assessment Matrix (see figure 4-4). The Risk Assessment Value will be used to prioritize hazards for risk mitigation actions and to group hazards into risk categorizes. The risk categories will be used to establish risk acceptance levels as follows. Risk Assessment Values 1-5 are unacceptable and mitigation actions must be taken immediately or operations terminated. Risk Assessment Values 6-9 are undesirable and require a decision by the Goddard Project Office to accept the risk. Risk Assessment Values 10-17 are acceptable with review by the GLAST LAT Instrument Project Manager. Risk Assessment Values 18-20 are acceptable without review.

Risk Assessment Values

SEVERITY PROBABILITY	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

MIL-STD-882D

Figure 4-4 Mishap Risk Assessment Matrix

4.2 System Safety Precedence

Risk management is a decision-making process consisting of evaluation and control of the severity and probability of a potentially hazardous event. By assigning a Risk Assessment Value, a determination can be made as to whether hazards should be eliminated, controlled, or accepted. The process shown in Figure 4-5 helps to determine the extent and nature of preventive controls that can be applied to decrease the risk to an acceptable level within the constraints of time, cost, and system effectiveness. Resolution strategies in descending order of precedence are listed below.

- Design to Eliminate Hazards This strategy generally applies to any change to equipment. The hazard source or the hazardous operation shall be eliminated by design without degrading the performance of the system.

- Design to Control Hazards In cases where hazards are inherent and cannot be eliminated completely, they will be controlled through design if possible. The major safety goal during the design process is to include safety features that are fail-safe or have capabilities to handle contingencies through redundancy of critical elements. Complex features that could increase the likelihood of hazard occurrence will be avoided wherever feasible. System safety analysis should identify hazard control, damage control, containment, and isolation procedures.

- Provide Safety Devices Hazards that cannot be eliminated through design will be controlled through the use of appropriate safety features or devices if possible. Safety devices (e.g. a pressure relief valve) that are part of the system, subsystem, or equipment, and are an integral part of emergency operations can result in the hazard being reduced to an acceptable risk level.

- Provide Warning Devices Where it is not possible to preclude the existence or occurrence of an identified hazard, visual or audible warning devices (e.g. a fire alarm bell) should be employed for the timely detection of conditions that precede the actual occurrence of the hazard. Warning signals and their application should be designed to minimize false alarms that could lead to secondary hazardous conditions.

- Provide Special Procedures or Training Where a hazard cannot be eliminated or controlled using one of the aforementioned methods, special malfunction or emergency procedures should be developed and formally implemented. These special operational procedures should be standardized and used in test, operational, and maintenance activities. For example, the user could be required to wear protective clothing or gear (e.g. face shields, gauntlets, etc.).

- Hazard Acceptance or Terminate System Where hazards cannot be reduced by any means, a decision process must be established to document the rationale for either accepting the hazard or for disposing of the system.

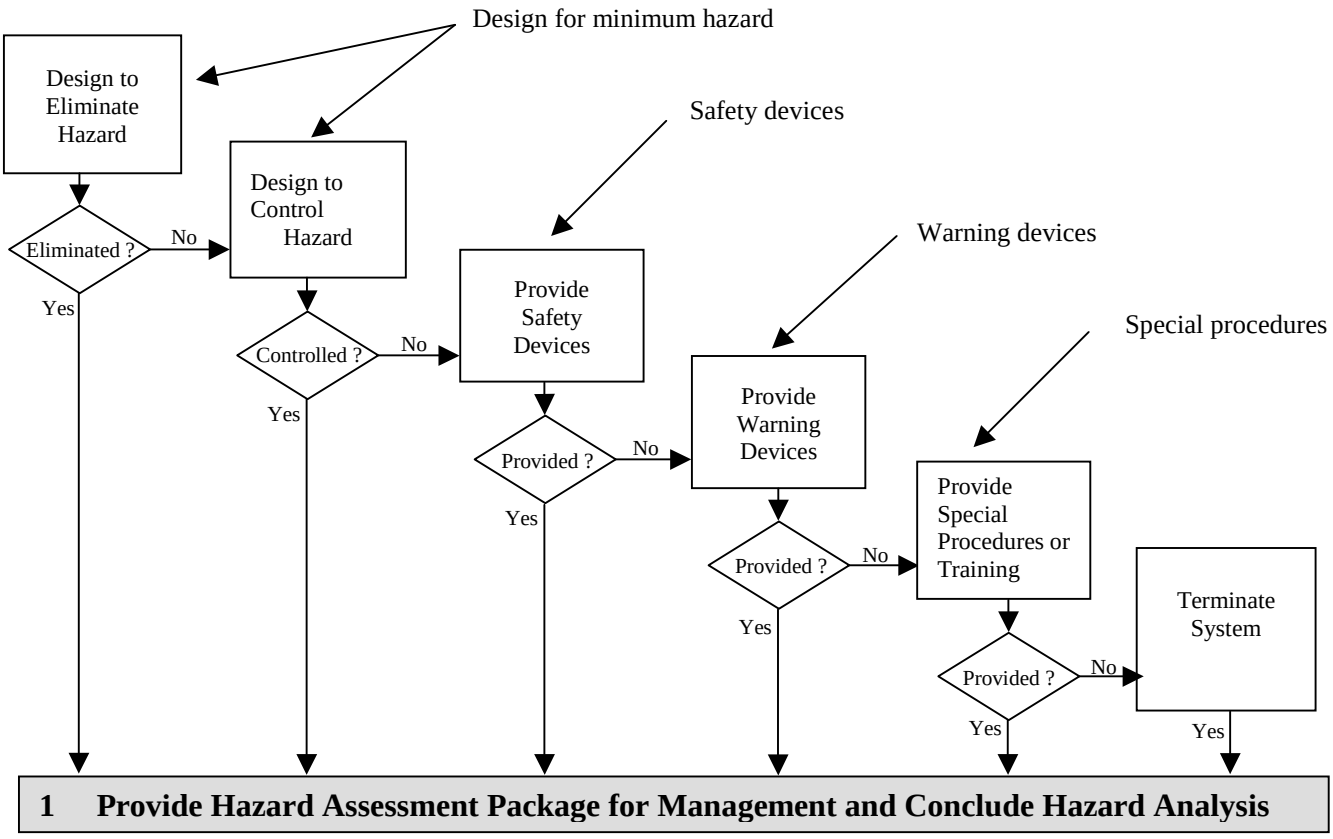


Figure 4-5 Hazard Reduction Precedence

4.3 Hazard Closure Criteria

Reduction of risk to an acceptable level will require verification that the necessary safety design and hazard control requirements have been implemented. Verification methods will include system safety review of specifications, drawings, and procedures; review of flight qualification and manufacturing acceptance test results; and inspections. Implementation of hazard controls will be documented in the PHA.

4.4 System Safety Analyses

A Preliminary Hazard Analysis (PHA), Operating and Support Hazard Analysis (O&SHA), and a Safety Assessment Report (SAR) will be performed and documented for the GLAST LAT. The PHA may identify additional analysis that should be conducted to identify hazards. The following is a description of the hazard analysis processes that are applicable during the design, development, integration, test, and operation of the GLAST LAT instrument.

4.4.1 Preliminary Hazard Analysis

The purpose of the Preliminary Hazard Analysis is to identify safety critical areas, provide an initial assessment of the hazards, and identify requisite hazard controls and follow-on actions. Based on the best available data, including mishap data from similar systems and other lessons learned, hazards associated with the proposed design or function will be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to Range Safety shall be included. A functional and physical description of the hardware will be included. The PHA will consider the following for identification and evaluation of hazards:

a. Hazardous components such as toxic substances, hazardous construction materials, pressure systems, and other energy sources

b. Safety related interface considerations among various elements of the system such as material compatibility, electromagnetic interference, inadvertent activation, fire initiation and propagation, and hardware and software controls

c. Safety design criteria to control safety-critical software commands and responses such as inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or designated undesired events shall be identified and appropriate action taken to incorporate them in the software and related hardware specifications

d. Environmental constraints including the operating environments such as drop, shock, vibration, extreme temperatures, humidity, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation

e. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures

f. Those test unique hazards that will be a direct result of the test and evaluation of the article

g. Facilities, real property installed equipment, support equipment such as provisions for storage, assembly, checkout, Proof testing of hazardous systems and assemblies that may involve toxic, flammable, corrosive or cryogenic materials and wastes; radiation or noise emitters; electrical power sources

h. Training and certification pertaining to hazardous and safety critical operations (such as lifting and handling) and maintenance of hazardous and safety critical systems

i. Safety related equipment, safeguards, and possible alternate approaches such as interlocks; system redundancy; fail safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers

j. Malfunctions to the system, subsystems, or software

4.4.2 Operating &Support Hazard Analysis

The purpose of the Operating and Support Hazard Analysis is to evaluate activities for hazards or risks introduced into the system by operational and support procedures and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks.

The O&SHA examines procedurally controlled activities. The O&SHA will identify and evaluate hazards resulting from the implementation of operations or tasks performed by persons, considering the following criteria: the planned system configuration and/or state at each phase of activity; the facility interfaces; the planned environments or the ranges thereof; the supporting tools or other equipment, including software controlled automatic test equipment, specified for use; operational and/or task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements; and the potential for unplanned events including hazards introduced by human errors. A functional and physical description of the ground support equipment will be included. The human will be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis.

The O&SHA will identify the safety requirements or alternatives needed to eliminate or control identified hazards or to reduce the associated risk to a level that is acceptable under either regulatory or Range Safety specified criteria. The analysis shall identify the following:

a. Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities and time periods

b. Changes needed in functional or design requirements for system hardware and software, facilities, tooling, or support and test equipment to eliminate or control hazards or reduce associated risks

c. Requirements for safety devices and equipment, including personnel safety and life support equipment

d. Warnings, cautions, and special emergency procedures such as egress, rescue, escape, render safe, explosive ordnance disposal, and back-out, including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication

e. Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials

f. Requirements for safety training and personnel certification

g. Effects of non-developmental hardware and software across the interface with other system components or subsystems

h. Potentially hazardous system states under operator control

4.4.3 Safety Assessment Report (SAR)

The purpose of the Safety Assessment Report is to comprehensively evaluate the mishap risk being assumed prior to test or operation of a system. The Safety Assessment Report will identify all safety features of the hardware, software, and system design and identify procedural, hardware and software related hazards that may be present in the system including specific procedural controls and precautions that should be followed. The safety assessment shall summarize the following information:

a. The safety criteria and methodology used to classify and rank hazards, plus any assumptions on which the criteria or methodologies were based or derived.

b. The results of analyses and tests performed to identify hazards inherent in the system, including:

1. Those hazards that still have a residual risk and the actions that have been taken to reduce the associated risk to an acceptable level.

2.Results of tests conducted to validate safety criteria, requirements and analyses

c. The results of the safety program efforts, including a list of all significant hazards along with specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment.

d. Any hazardous materials generated by or used in the system

e. The conclusion, including a signed statement, that all identified hazards have been eliminated or their associated risks adequately controlled.

f. Recommendations applicable to hazards at the interface of Range users systems with other systems, as required.

4.4.4 Hazard Control Verification Log

The purpose of the Hazard Control Verification Log is to establish a single closed-loop hazard tracking system in order to document and track hazards and their controls, providing verification of hazard resolutions. A centralized file, identified as the *Hazard Log* will be maintained and made available to Range Safety upon request. The Hazard Log will contain the following information:

a. Description of each hazard, including an associated risk assessment code

b. Status of each hazard and control

c. Identification of residual risk

d. Action persons and organizational element

e. The recommended controls to reduce the hazard to a level of risk acceptable to Range Safety

4.4.5 Ground Operations Plan Input

The purpose of the Ground Operations Plan Input is to provide a description of the hazardous and safety critical operations associated with the GLAST LAT. This input will include a description of hazardous operations and procedures that include hazardous tasks.

4.4.6 Safety Noncompliance Reports

Safety Noncompliance reports will be submitted to the Goddard Project Office if the GLAST LAT Instrument Project Office determines that it cannot meet the exact requirements of the range. All noncompliance reports will be submitted in accordance with the guidance provided in Appendix 1C of EWR 127-1.