

**LASER INTERFEROMETER GRAVITATIONAL WAVE
OBSERVATORY**

- LIGO -

CALIFORNIA INSTITUTE OF TECHNOLOGY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Document Type LIGO-M950046-D-M	10 September 2007
LIGO LABORATORY SYSTEM SAFETY PLAN	
LIGO Laboratory Directorate	

California Institute of Technology

LIGO Laboratory - MS 18-34
Pasadena CA 91125
Phone (626) 395-212
Fax (626) 304-9834
E-mail: info@ligo.caltech.edu

Massachusetts Institute of Technology

LIGO Laboratory - MS NW22-295
Cambridge, MA 01239
Phone (617) 253-4824
Fax (617) 253-7014
E-mail: info@ligo.mit.edu

www: <http://www.ligo.caltech.edu/>

CONTENTS

<i>AUTHORITIES</i>	1
<i>INTRODUCTION</i>	3
<i>PURPOSE</i>	4
SCOPE	4
OBJECTIVES	5
<i>APPLICABLE DOCUMENTS</i>	8
<i>SYSTEM SAFETY PROGRAM</i>	9
ORGANIZATION AND RESPONSIBILITIES	10
LIGO Laboratory Organization	10
System Safety Responsibilities	13
Integration & Coordination of Safety	14
Process for Management Decisions	14
SYSTEM SAFETY PROGRAM MILESTONES	16
SYSTEM SAFETY REQUIREMENTS	16
Work Permits	15
Risk Assessment	24
Reviews	27
Subcontractor Activities	28
Interfaces	29
Standards for Design and Operational Requirements	29
Documentation	29
HAZARD ANALYSES	30
HARDWARE/PERSONNEL PROTECTION	31
<i>SYSTEM SAFETY ASSURANCE</i>	32
PERSONNEL TRAINING AND CERTIFICATION	32
Training and Certification at LIGO	32
AUDIT PROGRAM	32
INDUSTRIAL/PUBLIC SAFETY	32
<i>ACRONYMS AND DEFINITIONS</i>	33
Standard Acronyms Used in System Safety	33
Definitions	34

LIST OF FIGURES

Figure 1: Aerial photograph of the LIGO Hanford Observatory. View is looking towards the SW, along the Y-arm. Two buildings are visible: one is at the 2 km midpoint; the other is at the 4 km terminus of the arm. The white structures along the arms are concrete covers protecting the vacuum tube. 3

Figure 2: LIGO Laboratory Incident Report Form 6

Figure 3: LIGO Safety Document Tree 6

Figure 4: LIGO Laboratory Organization Chart..... 11

Figure 5: LIGO Laboratory Safety Organization..... 12

Figure 6: Screen snapshot of Work Permit web form..... 19

Figure 7: System Safety Process Flow..... 19

Figure 8: Schematic of the Risk Matrix..... 23

LIST OF TABLES

Table 1: Hazard Severity Categories 22

Table 2: Hazard Probability Levels 24

Table 3: Hazard Risk Assessment Matrix..... 24

Table 4: Software Hazard Criticality Matrix. 27

LIGO Laboratory System Safety Plan

AUTHORITIES

Submitted by:

_____ Date _____

W. Tyler, LIGO Laboratory Safety Officer

Acceptance by:

MIT

_____ Date _____

David Shoemaker, Head, MIT LIGO Laboratory

LLO

_____ Date _____

Joe Giaime, Observatory Head

_____ Date _____

Rich Riesen, Observatory Safety

LHO

_____ Date _____

Fred Raab, Observatory Head

_____ Date _____

John Worden, Observatory Safety

Approved by:

_____ Date _____

A. Lazzarini, Deputy Director, LIGO Laboratory

INTRODUCTION

The Laser Interferometer Gravitational-Wave Observatory (LIGO) is distributed scientific facility poised to open a new observational window on the universe. LIGO is dedicated to the detection of cosmic gravitational waves and the harnessing of these waves for scientific research. It consists of two widely separated installations within the United States, operated in unison as a single observatory. This observatory is open for use by the international community and is the pioneer in a worldwide collaboration of gravitational-wave observatories.

To detect the very weak waves that are predicted requires two installations, each with a 1.22 meter (4-foot) diameter vacuum pipe arranged in the shape of an L with 4-kilometer (2.49-mile) arms (see *Figure 1* below). Since gravitational waves penetrate the earth essentially unimpeded, these installations need not be exposed to the sky and are entirely shielded by a concrete cover. At the vertex of the L and at the end of each of its arms are test masses that hang from wires which serve as reflecting mirrors. The main building at the vertex is the control center and houses vacuum equipment, lasers, and computers. Ultra-stable laser beams traversing the vacuum pipes measure the effect of gravitational waves on the test masses.

Figure 1: Aerial photograph of the LIGO Hanford Observatory. View is looking towards the SW, along the Y-arm. Two buildings are visible: one is at the 2 km midpoint; the other is at the 4 km terminus of the arm. The white structures along the arms are concrete covers protecting the vacuum tube.



Sited by the National Science Foundation (NSF), the installations were constructed near Livingston, Louisiana, and Hanford, Washington. The two sites, separated by slightly more than 3000 kilometers (approximately 2,000 miles), are both flat and large enough to accommodate the 4-kilometer interferometer arms. Both are also secluded from urban development to ensure an atmosphere of seismic and acoustic quiet, but still within convenient distance of housing for resident and visiting staff.

LIGO was designed and constructed by a team of scientists from the California Institute of Technology and the Massachusetts Institute of Technology. Small scale prototypes of laser-interferometric gravitational-wave detectors, and R&D laboratories operate at both institutions. LIGO is funded by the National Science Foundation (NSF).

PURPOSE

This document establishes the overall Safety Plan and governs procedures for conducting the LIGO Laboratory safety program. This system safety program provides a means to identify, eliminate or control safety risks and to provide an assessment of those risks. It further provides a management approach for assuring safe design and operations throughout all activities associated with the development and operation of LIGO.

This plan is the basis from which LIGO management can generate safety activities and/or plans which will assure an acceptable level of safety through interface evaluations, risk control, and reporting methods acceptable to the Laboratory and its oversight agencies. The LIGO safety activities are tailored to cost-effectively perform those tasks which are required to assure safety for personnel, equipment, and facilities throughout all phases of laboratory activities, including fabrication, installation, commissioning, and operations.

The total safety activity assures that an acceptable risk level is achieved by providing insight into the system design and installation activities, and that the LIGO Laboratory Directorate can certify that the operational system is safe to utilize. This will be accomplished by using a Work Permit process (refer to *Figure 6*). This process includes hazard identification, plans for hazard elimination or hazard control and the management/technical approaches used to minimize the risk of mishaps during the planned work.

SCOPE

Directions and guidelines for governing and evaluating overall Laboratory safety are provided in this System Safety Plan. Provisions are made for safety and interface activities involving, but not limited to, design, construction, fabrication, integration, commissioning, and science operations performed by the LIGO Laboratory, Caltech, MIT, and various contractors and subcontractors supporting LIGO. In addition, this plan is also applicable to any Laboratory furnished equipment or required support equipment, to the degree that any such equipment could affect the safety of personnel or critical hardware during integration, commissioning and science operation activities under the Laboratory responsibility.

It is understood that as the Laboratory matures and changes, safety needs and procedures will evolve. To ensure the viability of the Safety Plan, regular updates to this

document will be anticipated to most accurately reflect changes in priorities that match the design and operational practices, while assuring that all areas understand the impacts and are able to meet or provide the required safety support. The Safety Plan will be reviewed by the LIGO Safety Steering Committee and approved by the LIGO Laboratory Directorate and will be under document control.

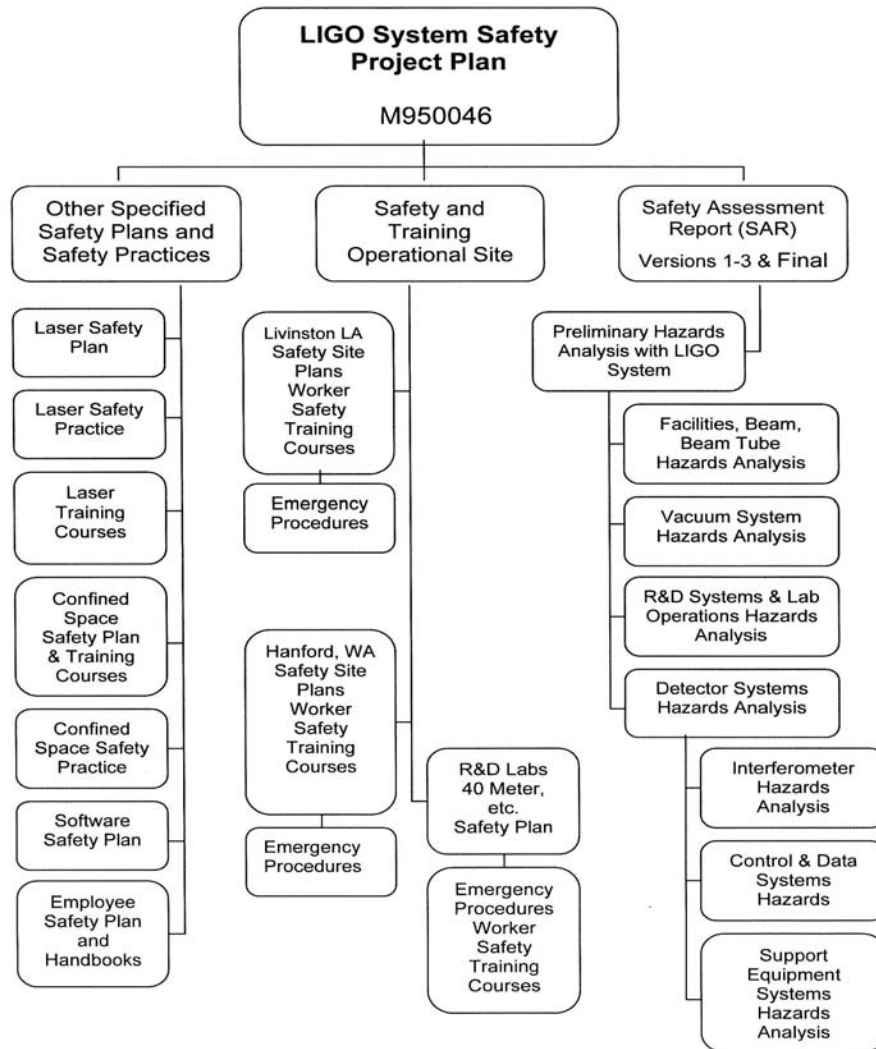
In all areas of fabrication, development, testing, handling, commissioning or operations of the LIGO system, subsystems or equipment, system safety is concerned with providing a program that is structured and managed to cover the following scope:

- Implementation of a Work Permit process for the identification and elimination/control of personnel or critical hardware safety hazards. This process includes a hazard analysis and, on safety critical items, developing and implementing appropriate (sub)system and operational hazard controls and procedures, as well as defining safety design criteria, verification tests, inspections, and assessment reports.
- Minimize mishap risk and prevent the occurrences of accidents resulting in personnel injury or death, catastrophic facility or equipment damage, or impede science data collection.
- Translate government imposed safety requirements into specific safety criteria, engineering requirements, and formal procedures.
- Disseminate safety information to appropriate design, engineering, operations, and program management organizations. Establish and maintain up-to-date safety training programs.
- Apportion the safety effort and resources in a manner commensurate with the magnitude of the hazards and risks to minimize costs and complexity.
- Establish and maintain an effective administrative procedure for incident reporting (Incident Report, refer to *Figure 2*), cataloging, tracking and resolving identified hazards and distributing “lessons-learned” information.

OBJECTIVES

The LIGO Laboratory Safety Plan documents requirements and defines the approach used to ensure safety for personnel, equipment, and facilities across all Laboratory activities with an acceptable risk consistent with Laboratory goals and resources. The objective of this safety implementation plan is to identify (1) the processes for determining the potential hazards associated with the LIGO Laboratory and (2) courses of action for reducing these hazards to an acceptable level. Further, this activity will be continuous, reviewed and modified as needed. The process results are the basis for generating the observatory/facility and laboratory specific Operational Safety Plans and the various Operational Safety Procedures that implement the risk reducing courses of action, to include corrective activities in the event of a mishap. Other documents generated from this process can be seen in the Safety Document Tree (refer to *Error! Reference source not found.*). This list of documents may is not exhaustive and will continue to be modified as the LIGO Laboratory system evolves.

Figure 3: LIGO Safety Document Tree



APPLICABLE DOCUMENTS

The operation of LIGO is the responsibility of the staff at Caltech and MIT under the terms of a Cooperative Agreement with the National Science Foundation (NSF). The safety documents containing requirements and/or guidelines for the LIGO Laboratory, its equipment and operations are listed below. The latest approved revision shall apply. The LIGO Safety Steering Committee may recommend additional documents as appropriate.

Federal Law

29 CFR Occupational Safety and Health

Administration (OSHA) General Industry Standards

49 CFR Department of Transportation (DOT)

Standards/Requirements

NFPA-75 – Fire Protection for Essential Electronic
Equipment

ANSI Z136.1 – Safe Use of Lasers

American National Standards Institute (ANSI)
Safety Standards

National Fire Protection Association (NFPA) Fire
Codes and Handbook of Fire Protection

Life Safety Code Handbook

National Electric Code (NEC)

Uniform Building Code (UBC), a national and
regionally applicable document for facilities

National Safety Council (NSC), Accident
Prevention Manual for Industrial Operations

Toxic Substances Control Act (TSCA)

Organizations/Guidelines

American Society of Mechanical Engineers

American Society of Steel Constructors

American Welding Society

SYSTEM SAFETY PROGRAM

Many of the resources for the application of system safety criteria to a program are drawn from existing source documents that promote the use of good design practices and the application of consensus standards to products or services. The application of such criteria is, in some cases, dictated by the law, and little discretion is left to the Laboratory or contractors. Examples are OSHA and DOT standards. In these cases the Systems Safety task is to research and apply these standards in a professional manner.

Application of consensus standards is not a guarantee of a safe environment, for two reasons. Consensus safety standards are written to address all possible situations, based on experience, but they cannot anticipate all environments and uses for a subsystem or instrument. In addition, all requirements must be interpreted and applied in an effective manner to meet the intent of the requirement. Requirements documents seldom explain the purpose of any particular requirement. Therefore, it is extremely important that every individual employed by or visiting LIGO (each staff member, student, employee and contractor) recognize that they are personally responsible for safety and following safe practices.

Other System Safety requirements may be identified by reviewing LIGO Incident Reports, past mishaps associated with the product or process or similar products or services and through other research related to the product or process or lessons learned. Risks and the means to eliminate them can also be derived from the analytical results of other disciplines, such as failure modes and effects analysis (FMEA) of human factors engineering.

System safety analysis and assessment provide the basis for the application of existing safety criteria or the derivation of new requirements. The application and interpretation of safety requirements, standards or principles to the design of a particular product, then, are not merely the research and application of written requirements. It requires the identification and interpretation of those requirements and the development of design/process solutions to apply the requirements. LIGO Laboratory has also implemented a Work Permit process to assure that review and hazard evaluation has been performed to ensure the design or process to be reasonably safe.

ORGANIZATION AND RESPONSIBILITIES

LIGO Laboratory Organization

The LIGO organization as a unit has the responsibility for the safe development, application of safety requirements, and operational safety of this system. The LIGO

Laboratory Directorate assumes the lead safety responsibility and has tasked the management organization (refer to **Figure 4**) to provide complete support in this endeavor. The LIGO Safety Officer has been designated the focal point and reports directly to the LIGO Laboratory Directorate on safety matters concerning operations, hardware, software, equipment, facilities or personnel.

Figure 4: LIGO Laboratory Organization Chart

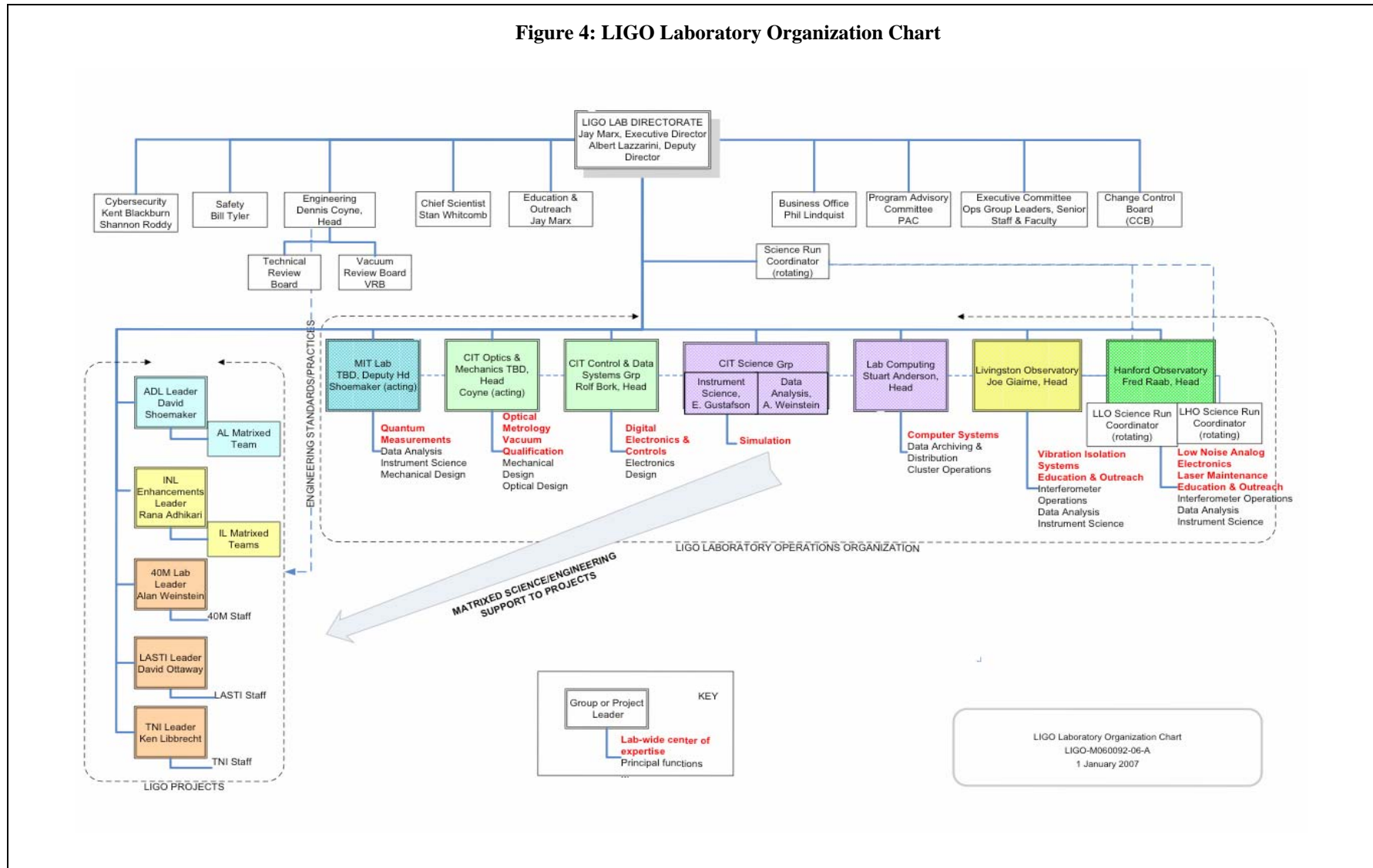
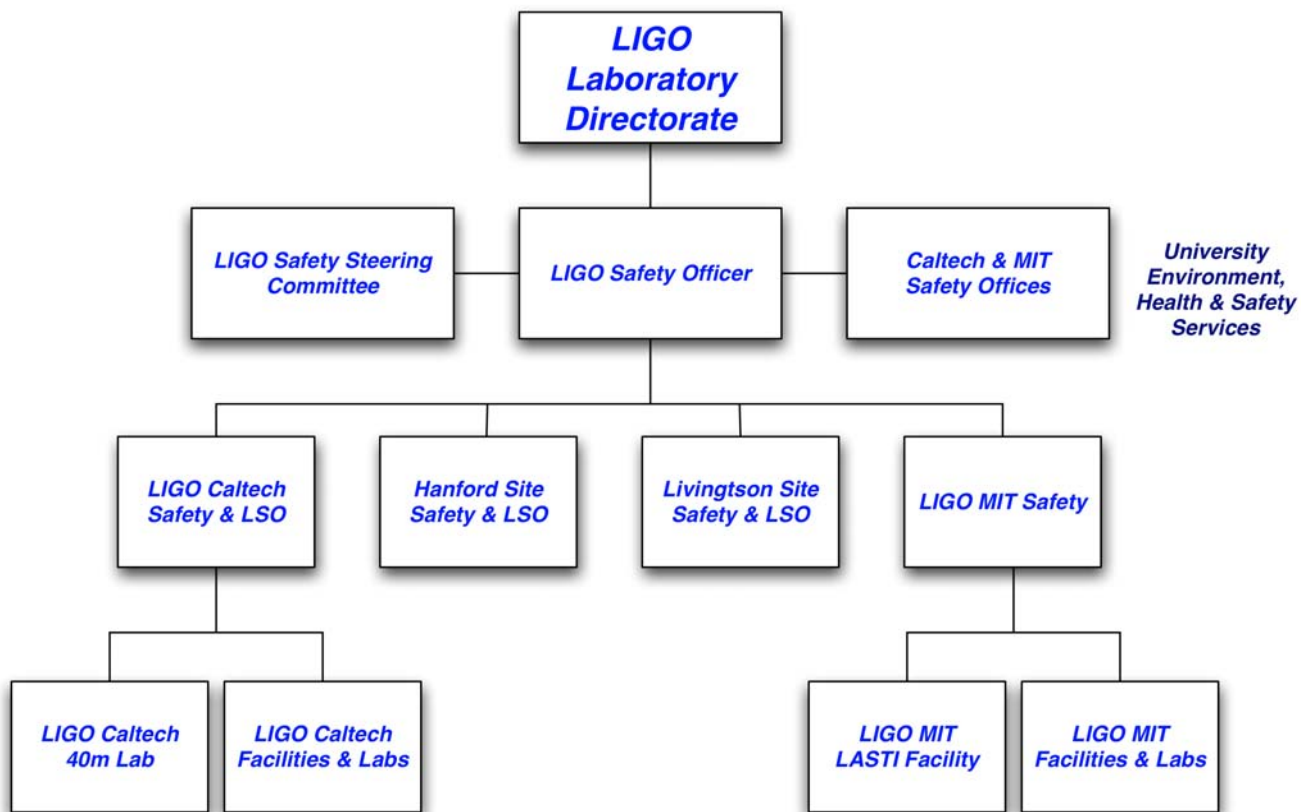


Figure 5:

LIGO Laboratory Safety Organization



Updated: 2007.05.08

System Safety Responsibilities

Internal

Everyone attached to LIGO (all staff members, students, employees and contractors) are personally responsible for safety and safe practices. All individuals must identify hazards and bring them to the attention of the Group Leaders, Safety Officer, or Laboratory Directorate.

The LIGO Laboratory organization consists of the Laboratory Directorate with support from key elements such as Safety Officer, Chief Scientist, Engineering and so forth. As shown in the organization chart (refer to *Figure 4*), these positions contain some overlap. Each element has different well-defined primary responsibilities.

The LIGO Directorate is responsible for the total safety performance of the Laboratory as shown in *Figure 5, LIGO Laboratory Safety Organization*, and is responsible for certifying that the LIGO System is safe for operation and science data gathering. The Deputy Director has been assigned the responsibility for safety activities and chairing the LIGO Safety Steering Committee (LSSC). The Directorate has the additional duty of assuring that the overall laboratory safety activities are properly organized and that the safety effort is proceeding effectively. Both the Executive and Deputy Director are fully informed on all major decisions and will be mutually involved in the decision making as appropriate.

The LIGO Safety Officer reviews and maintains current the Safety Plan and assures that the appropriate Laboratory safety activities are implemented. He/she reports to the Directorate and coordinates the LIGO Safety activities. He/she acts as a permanent member of the Safety Steering Committee and coordinates and/or audits safety activities of LIGO subcontractors and other outside agencies as appropriate. This Safety Officer will be the cognizant system safety representative for the LIGO Laboratory.

Therefore, the safety responsibility of the LIGO Directorate includes: (1) the design, manufacture and transport of hardware assembled and tested at Caltech (i.e. R & D equipment for lab testing) or the Observatories, (2) the monitoring of other contributing agencies for safety concerns during these phases, and (3) integration, commissioning and operation of the LIGO System in a safe fashion. MIT LIGO Laboratory Office will have a similar responsibility at the LIGO MIT labs and will be governed by LIGO Laboratory Safety Plans and procedures and must include the MIT site specific safety requirements for the MIT lab(s). However, any hardware or designs that are provided to or support the LIGO Observatories must meet the same safety requirements that the LIGO Directorate supports.

Outside Agencies

The LIGO Laboratory is operated in accordance with the Cooperative Agreement between NSF and Caltech. NSF is responsible for providing funding, general oversight, monitoring, and evaluation to help assure Laboratory performance in accordance with approved plans.

The LIGO Laboratory encompasses a joint effort of Caltech and MIT. The MIT roles and responsibilities are defined through a Memorandum of Understanding and subcontract with Caltech, updated as necessary. The MIT administration shares responsibility with the Caltech administration for overall oversight of the execution and performance of the LIGO Laboratory through representatives on the LIGO Oversight Committee. The MIT administration is also responsible for oversight, staffing and support of the MIT LIGO Group and for insuring that it successfully meets its institutional commitments, which includes responsibility and support of all safety requirements and policies of MIT. It is the policy of the LIGO Directorate to have a fully integrated MIT participation with institutional boundaries minimized.

Integration & Coordination of Safety

The procedures for integration and coordination of the system safety efforts, including dissemination of the system safety requirements to action organizations and contractors, along with generation and distribution of hazard analyses, is accomplished through the present Laboratory management organization as shown in *Figure 4*. Other official transfer of actions and coordination and safety information, shall occur during the program and design reviews, program status reporting, and the LIGO Safety Steering Committee (LSSC). The program and design reviews, program status reporting, and the LSSC shall also provide the closed loop feedback to assure that the actions requested were responded to in a timely and correct fashion.

Process for Management Decisions

The LSSC organization is used to advise the LIGO Directorate regarding safety issues and concerns and committee recommendations. This is a process used for identification of critical and catastrophic hazards, controls to eliminate or minimize these hazards, recommend corrective actions from review of Incident Reports, variance to safety requirements, and recommendations for personnel safety training.

LSSC Organization. The LIGO Deputy Director is the designated Chairperson, and with the Laboratory Safety Officer are permanent members of the Committee. The LSSC members are recommended by the LIGO Safety Officer and appointed by the LIGO Directorate. The members are drawn from all LIGO Laboratory sites. Degree of participation in the committee activities will be consistent with the hazards associated with the laboratory activity (including interfaces). As appropriate, additional consultants (i.e.: Radiation Safety Officer, Laser Safety Officer, specialty engineering people, etc.) may be appointed as members of the committee.

LSSC Meeting Schedule. The Committee will meet on a regular basis, as appropriate for Laboratory needs such as, when major modifications are in the planning phase, or at the request of the Chairperson. Group Leaders may request a committee review when they have a safety issue that involves interfaces outside of their organization, or if they wish to have an opinion on an issue that impacts their budget or schedule.

LSSC Duties. The Safety Steering Committee shall carry out the following duties:

- (1) Review and recommend the applicability of safety requirements for the LIGO Laboratory.
- (2) Perform a hazard review of the operational hardware, software, and support equipment designs as presented at Safety Steering Committee Meetings.
- (3) Evaluate techniques for minimizing or safely accommodating the hazards that cannot be eliminated.
- (4) Review hazard-related interfaces involving the operational hardware, support and handling equipment, facility complex, software, special materials, lasers, etc.
- (5) Evaluate integration, commissioning and operations schedules, and Work Permits, to assure appropriate personnel and equipment safety planning is included. Advise/recommend changes to Work Permits as required.
- (6) Review design changes which have safety implications and concur those changes are acceptable from a safety viewpoint.

The Chairperson of the Safety Steering Committee is responsible for:

- (1) Organizing, scheduling and conducting Safety Steering Committee and associated meetings.
- (2) Assigning action items or tasks to the members of the Committee or other Laboratory personnel, as necessary, to carry out Committee functions.
- (3) Assuring that the Committee work is carried out in a timely and effective manner.

The Laboratory Safety Officer, as a member of the Safety Steering Committee, is responsible for:

- (1) Supporting and advising the Chairperson in organizing meetings to carry out the duties of the Committee.
- (2) Assessing safety concerns regarding the interfaces between personnel, hardware, software, and/or equipment elements.
- (3) Acting as advisor for the Committee's activities in evaluating safety.
- (4) Coordination of Safety Steering Committee activities with the appropriate groups and outside agencies.
- (5) Acting as consultant to the Committee on safety matters, i.e. policy, requirements, standards, etc.

- (6) Suggesting areas for Committee evaluation and subjects for consideration.

SYSTEM SAFETY PROGRAM MILESTONES

The Chairman of the LIGO Safety Steering Committee and the Safety Officer will assure that necessary safety activities (e.g., meetings, safety reviews, the status of Work Permits and personnel safety training activities) are coordinated with the LIGO Laboratory milestones.

SYSTEM SAFETY REQUIREMENTS

In addition to the general requirements of the previous and following sections, the LIGO Laboratory must comply with safety requirements which are established by Caltech/MIT and external organizations such as OSHA, DOT, DOE, ANSI, etc. These deal with the following subjects:

- (1) Material design safety factors.
- (2) Safety mechanization of design (i.e., pressure relief mechanisms, emergency disconnects, etc.).
- (3) Safe use of lasers.
- (4) Determining when, where and how pressurized vessels, vacuum systems, cryogenics can be safely handled and/or operated.
- (5) Safe use of hazardous materials.
- (6) Electrostatic discharge safety requirements.
- (7) Confined space/limited access work areas.
- (8) Use of cranes and man-lifts.
- (9) High voltage personnel hazards.
- (10) Other appropriate safety concerns, as identified.

Work Permits

The Group or Project Leaders, working with the Observatory/Facilities Operations Manager and Safety Officer, prepares a Work Permit (refer also to **Figure 6**) for all significant activities requiring coordination of people or infrastructure use (independent of perceived risks in the process). The Work Permit documents all hazards or potential hazards associated with the planned work and methods to be used to eliminate and/or reduce the hazards to both personnel and hardware (refer also to *Error! Reference source not found.*, System Safety Process Flow). The potential hazards should be considered based on, but not limited to the following items:

- (1) System and subsystem affected.
- (2) Hazard definition, severity and category.

- (3) Hazard causes – include when and where these exist and influencing interfaces.
- (4) Applicable safety requirements.
- (5) Hazard controls – recommendations to eliminate, minimize or control hazard.
- (6) Safety Verification Methods – types of verification recommended.
- (7) Status of Verification – expected or required action completed with expected sign-off date to include types of approval expected.
- (8) Work Permit status will be periodically reported to the LIGO Safety Officer. Completed Work Permits will be submitted to the Document Control Center for cataloging and archiving.

The LIGO Safety Steering Committee may conduct periodic reviews of the LIGO Work Permits to determine that each hazard was identified and understood and that the appropriate level of safety methods/effort were exercised to provide an acceptable level of risk.

System Safety Design Requirements.

System safety design requirements will be specified after review of pertinent standards, specifications, regulations, design handbooks, safety design checklists, and other sources of design guidance for applicability to the system design. The LIGO Safety Officer, with the assistance of the LSSC, will establish safety design criteria derived from all applicable data including preliminary hazard analyses. These criteria shall be the basis for developing system specification safety requirements, using a typical system safety process flow as shown by *Figure 7*. The diagram is generic in nature, and is meant only to show the basic elements of the system safety process and the relationships of those elements. Some general system safety design requirements are:

- a. Eliminate identified hazards or reduce associated risk through design, including material selection or substitution. When potentially hazardous materials must be used, select those with least risk throughout the life cycle of the system.
- b. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.
- c. Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, cutting edges, or sharp points)
- d. Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).
- e. Design to minimize risk created by human error in the operation and support of the system.
- f. Consider alternate approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks, redundancy, fail safe design, system protection, fire

suppression, protective clothing, equipment, devices, and procedures.

- g. Protect the power sources, controls and critical components of redundant subsystems by physical separation or shielding.
- h. When alternate design approaches cannot eliminate the hazard, provide safety and warning devices and warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These shall be standardized in accordance with commonly accepted industry practice or with LIGO accepted requirements for conditions in which prior standards do not exist. The LIGO Safety Officer, the Directorate and the LSSC shall be provided copies of all warnings, cautions and distinctive markings proposed, for review and comment.
- i. Minimize the severity of personnel injury or damage to equipment in the event of a mishap.
- j. Design software controlled or monitored functions to minimize initiation of hazardous events or mishaps.
- k. Review design criteria for inadequate or overly restrictive requirements regarding safety. Recommend new design criteria supported by study, analyses, or test data.

Figure 6: Screen snapshot of Work Permit web form.

LIGO WORK PERMIT FORM

1. This is a beta product, please make suggestions (such as which documents are relevant for your facility)
[suggestions form](#)

2. work permit guidance: [M050194-00.pdf](#)

3. Facility: [???] ▾

4. Task leader: []

5. Facility liason (if different from task leader): [same](#) []

6. System, subsystem and location at facility:
 []

7. Activities to be performed:
 []

8. Relevant documents:
 please choose a site
 []
 Other Document Numbers:
 []

9. Hazards involved (ctrl-click all that apply):
 Electrical
 Eye
 Laser
 Crane
 Other hazards:
 []

10. Does this work require the use of a lock and tag? yes no

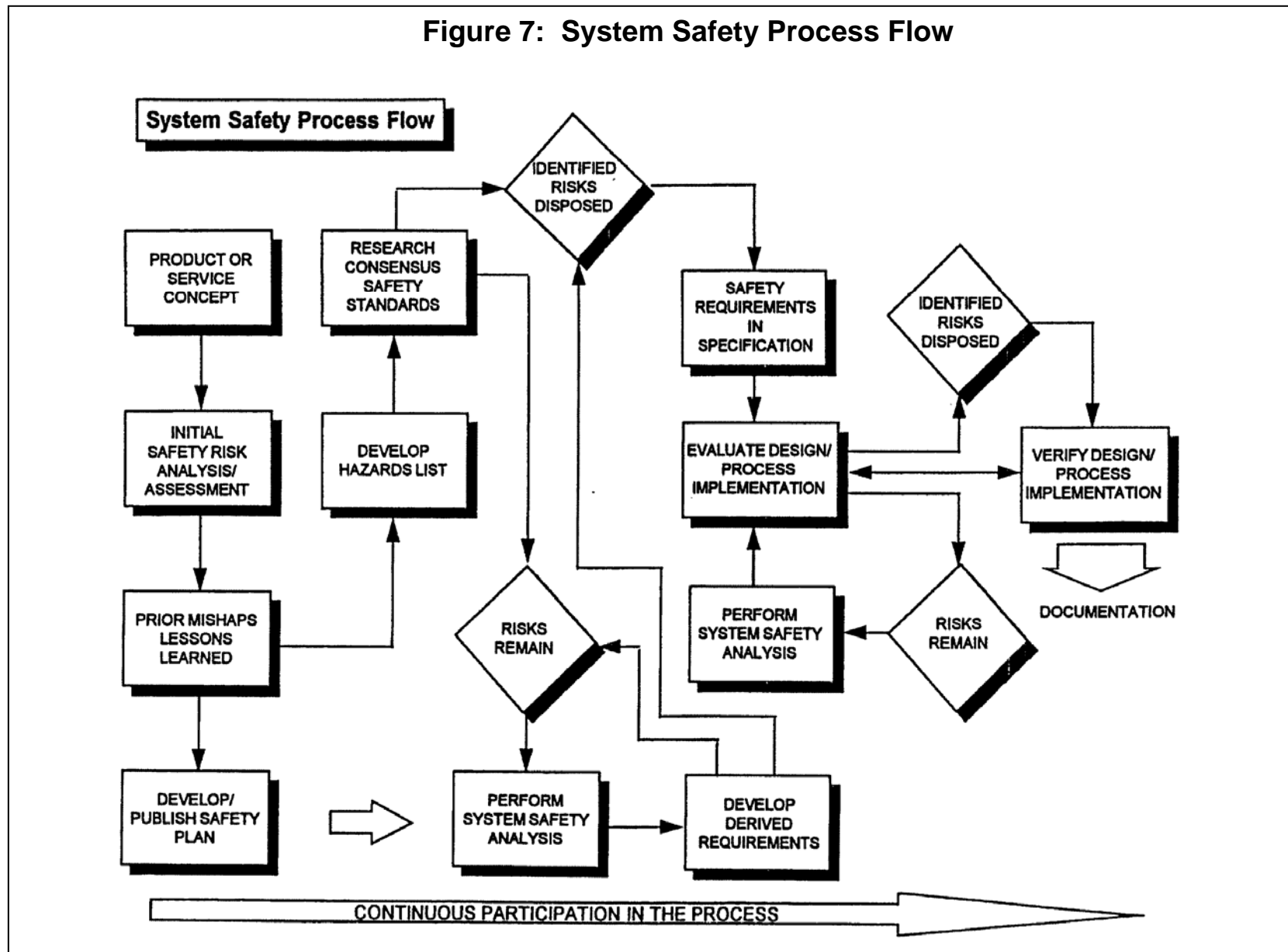
11. Does this work require the use of the buddy system? yes no
 Buddy: []

12. The work you are about to perform is: [Dangerous](#) ▾

13. Period of activity?
 begin: [] end: []

submit form

Figure 7: System Safety Process Flow



System Safety Precedence

The order of precedence for satisfying system safety requirements and resolving identified hazards shall be as follows:

Design for minimum risk. From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the Project/Group Leader, through design selection.

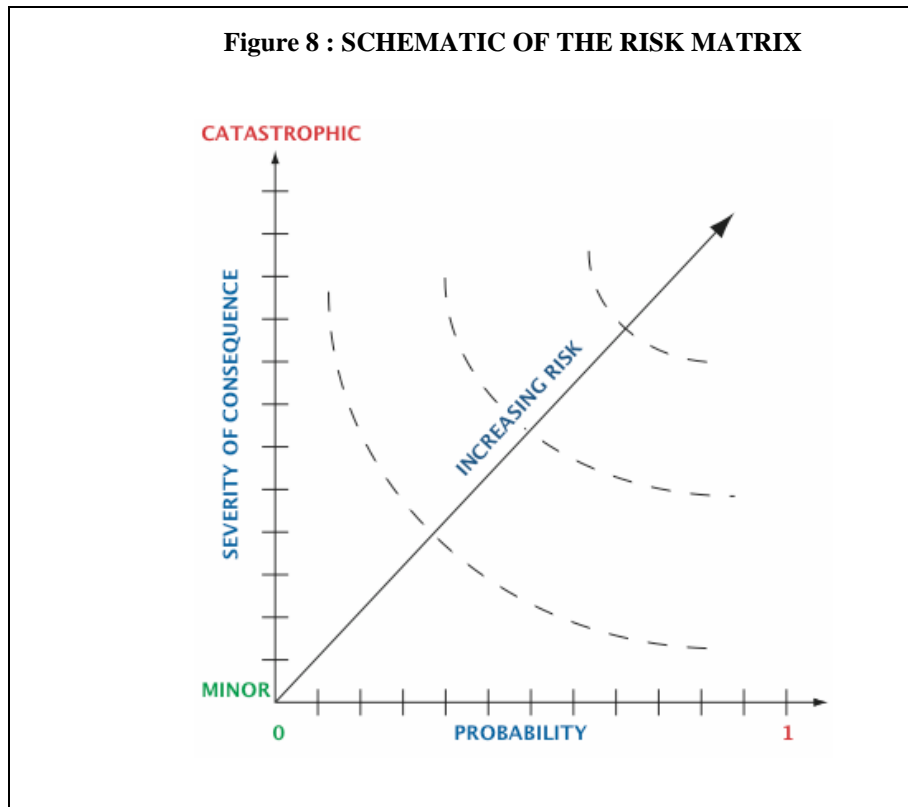
Incorporate safety devices. If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the Lab Directorate through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.

Provide warning devices. When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.

Develop procedures and training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific variance from the Lab Directorate, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category 1 or 2 hazards (see *Table 1*). Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the Lab Directorate. Tasks and activities judged to be safety critical by the Lab Directorate may require certification of personnel proficiency.

The Safety Officer will use various system safety analysis tools to identify the types of safety risks that can be anticipated as a result of the use of the system. Use refers to any environment the LIGO Laboratory may see during its life cycle. The initial development of the likely safety risks that are associated with a product or service is a matter of technical knowledge of the product as well as the application of the system safety discipline. *Figure 8* illustrates the risk concept using the elements of probability and severity to determine the acceptability of a particular safety risk. A catastrophic mishap can be acceptable if the probability of such a mishap is sufficiently low. Conversely, a higher probability of occurrence can be acceptable for a mishap that will not have serious consequences. The goal of the system safety task is to remain as close to the origin of the graph as possible.

<i>Table 1: HAZARD SEVERITY CATEGORIES</i>		
Hazard Severity	Category	Definition
Catastrophic	1	Death or permanent total disability, system loss, major property damage or severe environmental damage.
Critical	2	Severe injury, severe occupational illness, major system or environmental damage.
Marginal	3	Minor injury, lost workday accident, minor occupational illness, or minor system or environmental damage.
Minor or Negligible	4	Less than minor injury, first aid or minor supportive medical treatment type of occupational illness, or less than minor system or environmental damage.



Decisions regarding resolution of identified hazards shall be based on assessment of the risk involved. To meet the objectives of system safety, hazards shall be characterized as to hazard severity categories and hazard probability levels. Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction as shown in *Table 1*.

The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented for those operations or activities judged to be safety critical. An example of a qualitative hazard ranking is shown in *Table 2*.

Table 2: HAZARD PROBABILITY LEVELS

Probability	Level	Individual Item
Frequent	A	Likely to occur frequently or continuously experienced.
Probable	B	Will occur several times in the life of an item.
Occasional	C	Likely to occur some time 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 experienced.

Risk Assessment

Potential hazards identified through the hazard analyses are subject to a risk assessment procedure to establish priorities for corrective action. To aid in this assessment, each hazard is assigned a hazard severity category (*Table 1*) and a qualitative probability of occurrence (*Table 2*). The combination of hazard severity and probability can be displayed in a hazard risk assessment matrix (*Table 3*). The risk assessment code criteria (as shown in *Table 3*) provide the level of hazard acceptability by listing the management level of review required to accept the hazard.

Table 3: HAZARD RISK ASSESSMENT MATRIX

		HAZARD SEVERITY / CATEGORY			
		(1) Catastrophic	(2) Critical	(3) Marginal	(4) Negligible
PROBABILITY	(A) Frequent	1A	2A	3A	4A
	(B) Probable	1B	2B	3B	4B
	(C) Occasional	1C	2C	3C	4C
	(D) Remote	1D	2D	3D	4D
	(E) Improbable	1E	2E	3E	4E

Hazard Risk Index	Risk Code Criteria
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
1D, 2C, 2D, 3B, 3C	Undesirable (Directorate decision required)
1E, 2E, 3D, 3E, 4A, 4B	Acceptable with review by Directorate
4C, 4D, 4E	Acceptable without review

Software Risk Assessment Process.

The initial assessment of risk for software, and consequently software controlled or software intensive systems, cannot rely solely on the hazard severity and probability. Determination of the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application specific and reliability parameters associated with it cannot be estimated in the same manner as hardware. Therefore, another approach shall be used for the software risk assessment. It will consider the potential hazard severity and the degree of control that software exercises over the hardware. The degree of control is defined using the software control categories.

a. Software Control Categories.

I	Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a mishap. Failure of the software or a failure to prevent an event leads directly to a mishap occurrence.
IIa	Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.
IIb	Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the mishap occurrence.
IIIa	Software item issues commands over potentially hazardous hardware systems, subsystems or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.
IIIb	Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.
IV	Software does not directly control safety critical hardware systems, subsystems or components and does not provide safety critical information. However, software controls hardware/components that could indirectly affect safety critical hardware, propagating to a potential hazardous event. For example, fault recovery software might be triggered by failure of a non-safety critical component, resulting in temporary shutdown and reset of a control system which does control hazardous functions.

b. Software Hazard Criticality Matrix. The Software Hazard Criticality Matrix (*Table 4*) is similar to the Hazard Risk Assessment Matrix. The matrix is established using the hazard categories for the rows and the Software Control Categories for the columns. The matrix is completed by assigning Software Hazard Risk Index numbers to each element just as Hazard Risk Index numbers are assigned in the Hazard Risk Assessment Matrix. A Software Hazard Risk Index (SHRI) of “1” from the matrix implies that the risk may be unacceptable. A SHRI of “2” to “3” is undesirable or requires acceptance from the managing activity. Unlike the hardware related HRI, a low index number does not mean that a design is unacceptable. Rather, it indicates that greater resources need to be applied to the analysis and testing of the software and its interaction with the system.

Table 4: SOFTWARE HAZARD CRITICALITY MATRIX.

		CONTROL CATEGORY			
		I	II	III	IV
HAZARD CATEGORY	Catastrophic	1	1	2	3
	Critical	1	2	3	3
	Marginal	3	3	4	4
	Negligible	4	4	4	4

Software Hazard Risk Index (SHRI)		Suggested Criteria
1	High risk	Significant analysis and testing resources, may be required.
2	Medium risk	Requirements and design analysis and in-depth testing required, may require Management approval.
3	Moderate risk	High level analysis and testing acceptable with Managing Activity approval.
4	Low risk	Acceptable.

Reviews

To assure that the LIGO Safety program is vital and continues to maintain safety of personnel, equipment and facilities through all phases of projects, as well as ongoing Laboratory operations, the Laboratory Directorate may request an external agency perform annual safety reviews. This type of review compares the level of safety analyses, documentation, procedures, and verification of safety controls with the maturity of the program and science activity. The review shall evaluate the level of safety support and determine if the safety program is properly oriented to provide the maximum safety necessary to assure that potential mishaps are prevented by elimination or control of identified hazards. A secondary part of the review process is to determine if all hazards were identified, if risk assessments have been performed correctly with reasonable impacts projected and if hazards are properly controlled. By performing this type of

external check the Lab Directorate is assured that the LIGO Laboratory has made the best attempt at producing operationally safe Observatories.

When deemed necessary by the Lab Directorate, a readiness review of Work Permit(s), operating plans and/or test plans will be accomplished prior to the start of system or subsystem modifications, commissioning operations or tests of critical hardware. The review will be performed by an ad hoc committee appointed by the Lab Directorate and will meet to assure that the proposed Work Permit or operation plans meet the acceptability criteria of safety and readiness for the proposed work/operation.

Prior to the start of modifications, assembly or integration operations at the LIGO Observatories or facilities, safety inspections will be performed by a small group composed of representatives from the LIGO Safety Office and other personnel as deemed appropriate by the Observatory or Facilities Group Leader and/or the Laboratory Directorate.

Prior to the start of commissioning or science operations at the Hanford, Washington and Livingston, Louisiana Observatories, there shall be a review of the facility and/or operational safety program and procedures. Approval to start these operations is contingent upon a preoperational review and approval by representatives of all involved organizations to assure compliance with safety requirements.

Subcontractor Activities

It is the responsibility of each subsystem Group or Operations Leader at LIGO to obtain a proper safety plan from each of his/her subcontractors. To the maximum extent possible, existing contractor plans should be used. The subsystem Leader is also responsible for subcontractor safety evaluations, requirements, and controls. Responsibilities include activities such as furnishing safety requirements and interface information to the subcontractor and obtaining appropriate safety evaluations and reports from the subcontractor. The LIGO Safety Officer will review, comment on, and approve all Project contractually required safety plans for all contractors when their contents are considered acceptable. The cognizant subsystem Group Leader must also concur and provide formal document approval to the subcontractor by means of a letter from the LIGO procurement representative.

The LIGO contract manager must assure that, if required, the contract specifies or allows for, the delivery of safety data to verify equipment safety. Equipment verification data requests for safety certification must require that the applicable data is furnished to the LIGO Safety Officer to assure that sufficient information will be received to support the Lab Directorate safety evaluation in accordance with the Cooperative Agreement.

Safety requirements must be met on a schedule compatible with the overall LIGO schedule for meeting its safety obligations. Scheduled milestones such as safety reviews, data submittals, and verification procedures should be a part of safety planning in each area.

Interfaces

Numerous hazardous interfaces exist within the Observatory operational system. As requested by the Lab Directorate, members of the Safety Steering Committee will be requested to initiate actions and procedures to minimize and control these interface hazards; e.g., laser controls, vacuum pumps, servicing of the liquid nitrogen tanks, etc. The chair of the Safety Steering Committee will resolve problems associated with determining responsibilities for any hazardous interfaces between the systems, subsystems, or support equipment.

Standards for Design and Operational Requirements

Instructions to ensure safe operations are included as part of all new LIGO Laboratory organized project documentation; for example:

- (1) Design safety standards are a part of specification, review, and functional requirements documents.
- (2) Work Permits or Procedures containing hazardous operations are clearly marked in the text of the Work Permit or procedure where the hazardous events occur. The front covers of procedures should be marked in red “HAZARDOUS OPERATIONS.” Or, if none are contained, the front cover states in black print, “NO HAZARDOUS OPERATIONS.”
- (3) Operational safety constraints shall be included at the proper position in Work Permits or procedures and will be conspicuously marked.
- (4) Testing and commissioning safety requirements and constraints shall be included in the applicable test plans and procedures and will be conspicuously marked.

Documentation

This section describes those documents required to be prepared by the LIGO Laboratory for performance of the safety tasks. Other documentation requirements may be added as the Safety Steering Committee finds necessary. The proposed safety documents that will be generated to assure appropriate project safety requirements are shown in Figure 3 and selected documents are described as follows:

- (1) Safety Data Package (i.e. LIGO Safety Assessment Report) is prepared to obtain safety approval for initial (startup) operation of the LIGO Observatory system at Hanford, WA and Livingston, LA. It includes operational and laser systems and subsystem descriptions, safety matrices, hazards and their controls, materials lists, waivers, certificate of safety compliance, a handling/operational plan for the operational system handling and testing at the sites and all supporting information. Subsequent to the initial Observatory start of operations, safety assessment report updates will be issued and prepared by the LIGO Safety Officer using system and subsystem engineering inputs as requested by the Directorate.

- (2) Operating Plans and/or Procedures include test and operating plans and procedures to be used for the test/operation activity at Caltech (40 meter, etc.) and MIT (LASTI, etc.). LIGO-operated facilities, and for the operating sites/Observatories assembly, test, alignment and commissioning activities. These plans and procedures contain the necessary safety restrictions and directions to assure safety requirements are met. The necessary approval of such plans and for hazardous procedures at the sites will be by the LIGO Laboratory Directorate.
 - (a) Included under this category, a Site Initialization/Startup Procedure identifies hazardous operations during startup operations. Those items involving hazards shall be clearly marked in the initialization and startup sequence.
 - (b) Emergency Procedures address the types of plausible emergencies during each phase of the operations. The steps necessary to minimize injury to people and to prevent uncontrolled release of laser energy are described. Steps necessary to minimize damage to facilities and equipment are also described. The steps to be taken, the responsible people, involved emergency crews, equipment and facilities to be employed, etc., are included. The procedures will be reviewed and approved by the LIGO Laboratory Directorate as appropriate.
- (3) Contractor Safety Data are submitted by contractors building LIGO critical hardware to the Site Safety Officer and to the Directorate for safety review and approval. In the case of a piece part or other well established, simple piece of equipment, the Directorate may waive this requirement.
- (4) Other Laboratory Documentation Requirements include safety information such as Incident Reports, to be furnished as LIGO requirements dictate. The LIGO Safety Steering Committee may identify other documents required or needed to analyze or control hazardous activity.

Accident/incident investigations and reporting are in accordance with the applicable agency policy (i.e. OSHA, DOT, LIGO).

HAZARD ANALYSES

The LIGO Safety Steering Committee reviews the safety analysis of the operational systems and support equipment to determine the apparent hazard level. As the development progresses and as LIGO is revised and updated, the Committee assesses the possible need for more detailed safety analyses (other than the standard design analysis). The Safety Steering Committee requests from the Subsystem Project/Group or Technical Leader any new information or analysis required for complete understanding or control of any hazard. The Committee Chair assigns action items for performing any required analysis. Examples of techniques to be considered for such analyses are:

1. Fault Tree Analysis
2. Failure Mode and Effects Analysis
3. Energy Conversion Analysis
4. Time Sequencing Analysis
5. Software Safety Analysis

Contractors must provide assurance that their equipment or operations will not jeopardize personnel, LIGO equipment and facilities, or other support equipment. System safety encompasses all activities associated with the LIGO Laboratory, whether at the test facility, or contractor's facility, at the Observatory complex, during transport or during the initial startup and operational phase.

HARDWARE/PERSONNEL PROTECTION

To assure the safety of hardware and personnel, a LIGO Work Permit document will be prepared and approved for each location before the work/operation can start. The Work Permit will describe the planned work and identify and assess the potential hazards and safety risks and will identify methods for minimizing these safety concerns.

During facility commissioning and checkout, with various contractors on-site along with LIGO personnel, the LIGO Site Operational Safety document shall be the prime controlling safety document. On-site contractors must understand and integrate their safety systems to satisfy the LIGO Operational Safety requirements and procedures. When safety hazards are identified by either LIGO or contractor personnel that affect the safe operation between contractor safety procedures and LIGO Operational Safety requirements/procedures, LIGO staff shall have the authority and responsibility to cease all work in the affected area(s) until safe procedures can be generated and incorporated into both LIGO and contractor safety documentation. Such action may require LIGO and/or contractor personnel training and certification before work can be resumed.

When requested by the LIGO on-site manager or Laboratory Leader, one or more of the applicable safety surveys (operational, facility, transportation, or electro-static discharge) shall be conducted and documented prior to equipment transportation and/or beginning of site operational activities. The surveys shall be performed in accordance with the site specific operational safety document. LIGO Safety personnel shall conduct the surveys in conjunction with the agencies responsible for performing or supporting the activities. Discrepancies or outstanding issues shall be worked to the satisfaction of the LIGO Safety Officer. Surveys shall be performed sufficiently in advance of the planned activity to support correction of deficiencies without impacting the schedule.

SYSTEM SAFETY ASSURANCE

PERSONNEL TRAINING AND CERTIFICATION

The LIGO Safety Steering Committee will review areas needing personnel training and certification relating to hazardous operations. The Committee members assure that such requirements are met by the responsible organization.

Training and Certification at LIGO

This certification may include activities such as confined space access, crane operations, cryogenic loading, pressure system operations, equipment handling, storage, hardware removal/maintenance installation, laser equipment operations, commissioning and test operations. Training shall be done by organizations and personnel best qualified to do so and/or by organizations having operational responsibility. LIGO personnel safety training programs shall comply with OSHA, ANSI and other standards. The LIGO Safety Steering Committee will monitor the safety training programs and recommend changes, if needed, to the LIGO Safety Officer.

AUDIT PROGRAM

Each LIGO Safety Steering Committee member shall periodically survey the hazardous project activities under his/her responsibility. Each committee member is responsible for reviewing design and design changes, along with interfaces and interface changes, that may affect safety or cause a change in any hazardous condition or operation. Suspected changes in safety items or operations will be communicated to the Deputy Director and the Laboratory Safety Officer.

The LIGO Laboratory Safety Officer also overviews activities associated with the Operational and Commissioning activities. The Group or Project Leader may require/request special safety audits of any areas at his/her discretion. Formal reviews may serve as an audit if sufficient details of the hazardous activities and the safety precautions to be used are included as part of the review.

INDUSTRIAL/PUBLIC SAFETY

Industrial and/or public safety is part of the total consideration of safety activities under this plan insofar as they affect or are affected by project activities. These conditions include requirements of local, state, and Federal governments, regarding such items as design and maintenance of facilities, test constraints, transport and storage of hazardous items, etc.

ACRONYMS AND DEFINITIONS

Standard Acronyms Used in System Safety

The acronyms listed below are used in System Safety, although are not necessarily referenced in this Plan.

DOD	Department of Defense
DOT	Department of Transportation
EPA	Environmental Protection Agency
HRI	Hazard Risk Index
OSHA	Occupational Safety and Health Administration
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
SCCSC	Safety Critical Computer Software Components
SDR	System Design Review
SHA	System Hazard Analysis
SHRI	Software Hazard Risk Index
SRR	System Requirements Review
SRS	Software Requirements Specifications
SSG	System Safety Group
SSHA	Subsystem Hazard Analysis
SSPP	System Safety Program Plan
TBD	To be Determined

Definitions

These are common definitions presently supported by System Safety.

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

Contractor. A private sector enterprise engaged to provide services or products within agreed limits specified by a contract and/or statement of work.

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, handle or dispose.

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.

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 component, or assembly.

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.

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 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.

System safety 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 project managers.

System safety program plan. A description of the planned tasks and activities to be used 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