LASER INTERFEROMETER GRAVITATIONAL WAVE OBSERVATORY

- LIGO -

CALIFORNIA INSTITUTE OF TECHNOLOGY

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Document LIGO-M070360-04-M **6 February 2008**
Advanced LIGO Safety: Processes and Guidelines
David Shoemaker

Distribution: LSC Advanced LIGO team

This is an internal document of the Advanced LIGO Project.

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/

PURPOSE

This document summarizes the operational elements of the LIGO System Safety Plan (LIGO-M950046, most recent version) for Advanced LIGO and provides guidance on how to ensure safety for the Advanced LIGO design, prototyping, fabrication, and installation. The LIGO System Safety plan always takes precedence over this document.

SCOPE

This document is intended to address safety concerns, and opportunities to design in safety, for Advanced LIGO. Once the responsibility for equipment is taken from Advanced LIGO by the Observatories, this document is no longer relevant. It is designed to complement the System Safety Plan.

OBJECTIVES

The objective of this safety implementation plan is to identify (1) the potential hazards associated with the Advanced LIGO designs (in assembly, installation, testing, and operation) and (2) courses of action for reducing these hazards to an acceptable level through appropriate design decisions, documentation, and operational procedures.

ACTIONS

1) All Advanced LIGO Subsystem Leaders and Cognizant scientists/engineers must read this document, and follow these guidelines for their subsystems. All Subsystem Leaders must ensure (and take the responsibility) that the people working on their subsystems are aware of any relevant hazards and risks, and plans for mitigation, and applicable procedures.

2) All Advanced LIGO subsystems must either develop Hazard Analyses for their subsystem per the instructions in this document, or request a waiver due to either lack of perceived Hazards or only a need for standard precautions. If a Hazard analysis is needed, it must be reviewed and approved before any activity with non-negligible risk takes place.

3) Procedures for assembly/test/installation will, in general, be needed to lead people safely through those activities and represent part of a complete plan for safety. The procedures should reflect the hazard analysis. If the subsystem could present a safety hazard in normal operation, a Standard Operating Procedure which addresses these hazards is also required.

4) All participants in any phase of Advanced LIGO – design, fabrication, assembly, installation, or test – are to be encouraged to mention either risks they see or solutions to reduce risk. All concerns raised must be tracked and considered by the Subsystem Leader or delegate, and either accommodated or clarified as not a risk to the person who raised the issue.

APPLICABLE DOCUMENTS

LIGO System Safety Plan (LIGO-M950046, most recent version)

Example Hazard Analysis: E070201 ELIGO FR Magnet Assembly Hazard Analysis, most recent version

Advanced LIGO safety organization

Advanced LIGO is a 'matrixed' project taking place within the LIGO Laboratory Organization. Safety in any LIGO activity is always ultimately the responsibility of the LIGO Laboratory Directorate. However, during the Advanced LIGO Project, there is also a chain of responsibility which passes through the Advanced LIGO Project organization. Specifically,

- The Advanced LIGO Leader has responsibility for the safety of the designs and the individuals working in Advanced LIGO until the equipment and procedures are accepted by and formally signed over to the designated site safety individual. Advanced LIGO will have a safety officer, who reports to the Advanced LIGO Leader and works closely with the LIGO Laboratory Safety Officer. S/He will help the Advanced LIGO Leader to make Advanced LIGO as safe as reasonably possible.

- Safety in Advanced LIGO is to be considered during the design process (to 'design in' safety), and then for the 'activity safety' during the prototyping process, the fabrication, assembly, installation and subsystem test process, and during the commissioning.

- Advanced LIGO will include safety considerations in the subsystem documentation, requiring a Hazard analysis of all aspects of Advanced LIGO. The Subsystem Leaders are responsible to present this document and own the contents. The level of detail and the focus will evolve with the phase of design, and with the nature of the specific components/activities, but all aspects must be satisfactorily addressed by the Final Design Review.

- Reviews of Advanced LIGO subsystems will include the LIGO Laboratory safety officer or his/her designate, and all concerns raised by that person will be resolved before either the next review stage or before that safety hazard would be realized (in e.g., a prototype experiment)

The Hazard Analysis

Is a Hazard Analysis needed? Consider the subsystem or component activity (assembly, installation, test, operation). Are there activities which could lead to personal injury? Are any of these hazards ones which are not covered by standard Laboratory practice for laser, electrical, mechanical, chemical, or software activities? If so, a Hazard Analysis is needed.

If not, then the relevant procedure must contain in its first paragraph references to any relevant standard Laboratory safety documents (e.g., laser SOPs, crane usage, chemical usage, software coding standards), and any hazardous steps in the procedure noted with the word '**Hazard'** in boldface type.. A request must be made via email to the Advanced LIGO Leader (responsible for safety) with a brief description of the activity and the explanation for exemption from the need for a Hazard Analysis, and a positive response is needed before undertaking that procedure for the first time.

If a Hazard Analysis is needed: The subsystem, or component, Hazard Analysis will include the following headings:

- **Summary** providing a synopsis of determinations and identifying the most severe level of hazard found, and whether it requires Directorate action (see below for this threshold)

- **Scope** of this analysis, including a self-contained concise description of the equipment/software. The subsystem leader will determine the appropriate approach to dividing the subsystem for safety issues.

- **Interfaces** to the scope treated in this analysis – can refer to design documentation

- **Related documents** – subsystem/component documentation, hazard analyses for interfacing systems, over-arching documents on e.g., laser safety, etc.

- **Hazard severity table**

The Hazard severity table will be built as an Excel spreadsheet and incorporated into the Microsoft Word document, with the columns labeled *Hazard, Cause, Effect, Severity, Level, Risk*, and *Comment*. Additional columns to the right of the required columns are welcome to supplant this information, and/or to help track the mitigation of the hazards. The Excel sheet and Word sources will be archived in the DCC along with pdf versions.

A signature sheet is needed, with the following signatories indicated:

- Subsystem leader

- Site safety responsible

- Advanced LIGO Systems Engineer

- Advanced LIGO Leader

- LIGO Laboratory Safety Officer

- LIGO Laboratory Deputy Director

Once a draft of the Hazard Analysis has been developed,

- It should be shared with other engineers and scientists familiar with the system, and interfaces, as a quality check. Those signing should review and comment.

- It must be shared with the Laboratory Safety Officer (Jan2008: Bill Tyler) for his cross-check and flags of hazards which require Directorate sign-off.

- It must be circulated to the Deputy Director (Jan2008: Albert Lazzarini) for his comments.

- The signature page must be completed by the appropriate individuals.

- Lastly, all individuals involved in the activity must be provided with a pointer or a walk-through by a supervisor of both the procedure in question and the Hazard Analysis.

Hazards must 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. 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. The appropriate hazard ranking is shown in ***Table 2***.

Table 1: HAZARD SEVERITY CATEGORIES

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 dam
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.

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 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

All hardware subsystems must consider at least the following factors in their considerations of hazards, and address those which are relevant.

(1) Material design safety factors

(2) Safety mechanization of design (i.e., pressure relief mechanisms, emergency disconnects, etc.)

(3) Safe use of lasers

(4) Design and use of pressurized vessels, vacuum systems, cryogenics

(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

and any other appropriate safety concerns, as identified.

Numerous hazardous interfaces exist within the Observatory operational system, e.g., laser controls, vacuum pumps, servicing of the liquid nitrogen tanks, etc. Advanced LIGO Subsystem Leaders must ensure that safety aspects of these interfaces are properly addressed in the design, documentation, and at the time of subsystem reviews, and acknowledged in the Hazard Analysis.

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.

Table 4: *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.

Software Hazard Criticality Matrix. The Software Hazard Criticality Matrix 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 5: *Software Hazards*

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

At each Advanced LIGO review (DRR, PDR, FDR) the status of safety plans will be assessed. All subsystems, whatever their state of development, must prepare a Hazard Analysis; it may be preliminary and incomplete at early design phases, but anticipated hazards should be indicated. The document is expected to be revised for subsequent reviews.

A readiness review of Hazard Analyses, Work Permit(s), operating procedures and test plans will be accomplished prior to the start of any activity with risks other than those indicated as 'negligible'. Advanced LIGO requires such a review; in parallel, the Lab Directorate may also wish a review. The objective is to assure that the proposed Work Permit or operation procedures meet the acceptability criteria of safety and readiness for the proposed work/operation.

Similarly, 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 Advanced LIGO management, and others as determined by the Lab Directorate.

Subcontractor Activities

It is the responsibility of each subsystem Contracting Officer's Technical Representative (COTR) 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 COTR 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

relevant COTR must also concur and provide formal document approval to the subcontractor by means of a letter from the LIGO procurement representative (Contracting Officer or CO).

The LIGO COTR and CO 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 Advanced 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.

Work Permits

The Group or Project Leaders, working with the Observatory/Facilities Operations Manager and Safety Officer, prepares a Work Permit 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.

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.