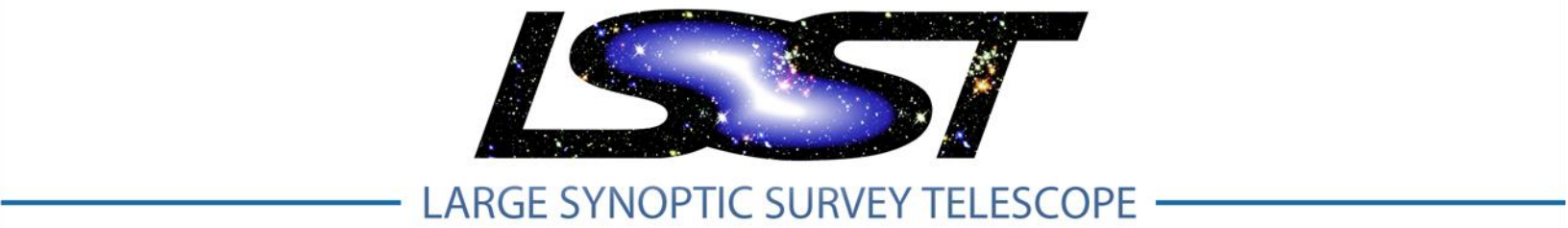

Large Synoptic Survey Telescope (LSST)

LSST Hazard Analysis Plan

Chuck Gessner, Victor Krabbendam, F. O'Neill

LPM-49

Latest Revision Date: September 29, 2014

Change Record

Version	Date	Description	Owner name
1	1/31/2011	Initial Version	C. Gessner
2	3/21/2011	General Updates	J. Sebag
2.1	9/30/2013	Inter-document consistency check. LSSTC-AURA correction, typos. No content changes. Approved under LCR-154	R. McKercher
	10/4/2013	Implementation of LCR-154	R. McKercher
	4/2/2014	Residual risk addition	C. Gessner and F. O'Neill
3	9/28/2014	Implementation of LCR-173 re: Residual Risk	R. McKercher

Table of Contents

The LSST Hazard Analysis Plan

Summary

Hazard analysis is a critical element of system safety. This LSST Hazard Analysis Plan describes the LSST Project's implementation of an ongoing hazard analysis process through the construction, commissioning, and operations phases of the project.

Acronyms and Definitions of Terms

- Glossary of Abbreviations (Document-11921)
- Glossary of Definitions (Document-14412)

Reference Documents

- LSST Safety Policy (LPM-18)
- U.S. Department of Defense MIL-STD-882D w/CHANGE 1, *Standard Practice for System Safety* (Draft, 29 March 2010)

The LSST Hazard Analysis Plan

1 Introduction

The Large Synoptic Survey Telescope (LSST) project is committed to developing a system that is safe to construct, commission, operate and maintain. This Hazard Analysis Plan defines the formal methodology undertaken throughout the project to analyze systems and to identify, mitigate and otherwise manage all risks of harm to equipment, personnel and the environment. This plan conforms to the objectives and requirements established in the LSST Safety Policy (LPM-18).

LSST has adopted a variation of the U.S. Department of Defense MIL-STD-882D w/CHANGE 1, *Standard Practice for System Safety* (Draft, 29 March 2010) for identifying and managing hazards during all phases of the project from conceptual design through construction and into operations. Central to the process outlined in MIL-STD-882D is the concept that analysis begins in the earliest phases of a project, starting as soon as elements of a conceptual design exist. Hazards must be identified, ranked and mitigated.

Hazard analysis is a critical element of system safety, and is the topic of this LSST document. This document describes the LSST project's implementation of an ongoing hazard analysis process through the construction, commissioning, and operations phases of the project.

2 Definition of Terms

The MIL-STD-882D w/CHANGE 1 ("Standard") establishes careful and precise definitions for 54 terms it uses; however, the following six are sufficient to understand this summary. While the Standard lists the terms in alphabetical order, here they are listed in a logical development where the first few, at least, don't require a precise understanding of other definitions to follow.

2.1 System

"The organization of hardware, software, material, facilities, personnel, data, and services needed to perform a designated function within a stated environment with specified results, such as the gathering of specified data, data processing, and delivery to users."

This is a somewhat broader definition of system than commonly used by telescope systems engineers, with its greater emphasis on people and process, but the additional emphasis is important for safety-related analyses.

2.2 Lifecycle

"All phases of the system's life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal."

In practice for LSST, this is being accomplished by defining phases of the life cycle, which include:

- Design and Development (D&D): includes all pre-construction activities
- Construction (CONST): includes fabrication and site construction activities

- Commissioning (COM): includes integration and test on site and science verification
- Operations (OPS): includes all operational activities and regular maintenance, troubleshooting and servicing.
- Disposal (DISP): includes decommissioning and dismantling of the facility. Disposal is a particular phase that is addressed specifically through dedicated comprehensive planning. The LSST Hazard analysis identifies hazards in the Disposal phase however, this effort does not constitute a comprehensive assessment during this final de-commissioning activity.

2.3 Mishap

"An unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. For the purposes of this document, the term "mishap" includes negative environmental impacts from planned and unplanned events and accidents."

The LSST hazard analysis must take into account three classes of classical mishaps and one non-traditional operational mishap:

- Personnel death, injury or occupational illness;
- Damage to or loss of equipment or property;
- Damage to the environment;
- Operational mishap.

The Standard does not explicitly consider an event that causes lack of availability of a system (i.e. "downtime") to be a mishap. For example, a high-humidity event that causes water to condense on the primary mirror surface requiring downtime to wash the mirror is not considered a mishap. As inconvenient as the event may be, no one was injured; no equipment was permanently damaged, nor was the environment negatively impacted. Nevertheless, events causing operational losses still can be included in the analysis without contravening any of the basic principles of the Standard.

2.4 Hazard

"A condition that if triggered by one or more causal factor(s) can contribute to or result in a mishap."

The difference between a hazard and a mishap, therefore, is that a hazard represents a potential for a negative event while a mishap is the realization of that event.

There may be hazards associated with the early moments of a power failure if systems have not been designed to fail safely, but once the observatory is in a benign (though non-operational) state with flashlights issued to all, a condition that results in the temporary inability to do physics is not, by this definition, a hazard.

2.5 Risk

"A measure of the potential loss from a given hazard. Risk is a combined expression of the severity of the mishap and the probability of the causal factor(s)."

The Standard eventually establishes a means of assigning a numerical value to this "expression" allowing a formal and common ranking of the hazards.

2.6 System Safety

"The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system lifecycle."

With this definition in place it is possible to understand the meaning of the title of the Standard: *Standard Practice for System Safety; Environment, Safety, and Occupational Health Risk Management Methodology for Systems Engineering.*

3 Identification of Hazards

The first step in the hazard analysis is to: *"Identify hazards through a systematic hazard analysis process that includes system hardware and software, system interfaces, the environment, and the intended use or application. Consider and use mishap data; relevant environmental and occupational health data; user physical characteristics; user knowledge, skills, and abilities; and lessons learned from legacy and similar systems. The hazard identification process shall consider the entire system lifecycle and potential impacts to personnel, infrastructure, the public, and the environment. As hazards are identified, they are entered into the hazard tracking system."*

One critical element of this formal process is careful documentation. The LSST project uses a common spreadsheet to contain the identification, the hazard assessment, and mitigation plans and approaches. The spreadsheet is found in Appendix A. Each of the main subsystems, using dedicated worksheets maintains this hazard table.

3.1 Hazard Number

Each identified hazard is assigned a unique identifier that begins with a subsystem code followed by a sequential number (e.g. M1M3-43). During the course of the process identifiers are not reused.

3.2 Machine or Sub-Process

This space is used for a precise description of the process or for expanding on the location associated with the hazard.

3.3 User

This column is used to indicate the type of personnel that could be involved with this hazard.

3.4 Task Description

This column describes the task during which the hazard exists.

3.5 Hazard Category

The hazard category is identified by a single word chosen from a common general list.

3.6 Hazard

The hazard column is used to specify the class of hazard. Some common examples include

- Pinch hazard;
- Collision hazard;
- Fall hazard; and
- Spill hazard.

3.6.1 Cause or Failure Mode

This column lists the circumstances or conditions that would lead to a mishap.

3.7 Project Phases

The hazard analysis will be used throughout the project and will address hazards in all phases of the project. This field is used to indicate the phases associated with each identified hazard as stated in section 2.2. The term "All" is used when the hazard could happen during construction, integration, maintenance and operations.

3.7.1 Comments

The Comments column can be used during any part of the process to add additional explanations, to pose questions for additional study, or make other notes pertinent to the hazard.

4 Risk Estimation

The quantitative estimation of the risk is made relatively easy by the very specific process and guidelines set out in the Standard. In summary, each risk is ranked based on two criteria: the severity of the problem, and the likelihood.

4.1 Severity

The severity of a mishap is ranked into one of four well-defined categories:

1. Catastrophic – Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or property loss exceeding $10M.
2. Critical – Could result in one or more of the following: permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, reversible significant environmental impact, or property loss exceeding $1M but less than $10M.

3. Marginal – Could result in one or more of the following: injury or occupational illness resulting in 10 or more lost workdays, reversible moderate environmental impact, or property loss exceeding $100K but less than $1M.
4. Negligible – Could result in one or more of the following: injury or illness resulting in less than 10 lost workdays, minimal environmental impact, or property loss less than $100K.

The explanation included with each category takes much of the potential subjectivity out of the analysis. Once the hazard is understood it takes little or no discussion to decide what rank it deserves. The amount of monetary losses permissible for each level of severity must be adjusted to the size of the system and actual financial impact, and must be routinely updated to reflect current replacement or indemnification costs, and changing economic environment.

4.2 Probability

Similar detailed criteria are provided for six measures of the probability of a mishap:

A. Frequent – Likely to occur often in the life of an item; with a probability of occurrence greater than 10^{-1} in that life.
B. Probable – Will occur several times in the life of an item; with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.
C. Occasional – Likely to occur sometime in the life of an item; with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.
D. Remote – Unlikely, but possible to occur in the life of an item; with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.
E. Improbable – So unlikely, it can be assumed occurrence may not be experienced in the life of an item; with a probability of occurrence of less than 10^{-6} in that life.
F. Eliminated – Incapable of occurrence in the life of an item. This category is used when potential hazards are identified and later removed or eliminated after the mitigation actions are in place.

NOTES:

I. Use either the quantitative or qualitative descriptions of probability, as appropriate, for a given analysis.
II. Use either the individual item or fleet inventory description, depending on which description produces the more frequent probability level for a given analysis.
III. Probability level F is reserved for cases where the causal factor is either no longer present or it is impossible to lead to the mishap. No amount of doctrine, training, warning, caution, personal protective equipment (PPE), or other change can move a mishap probability to level F.
IV. The probability of occurrence may have to be adapted to what's acceptable, tolerable or legally mandated for a given system.

If the hazard is well understood and rankings are established by a group having experience with the environment and materials, there should be a quick consensus about what ranking a hazard is given.

Once severity and probability rankings are established for a hazard, the remaining columns of the hazard analysis form can be completed. These are risk index and risk level, which are both discussed in the following sections.

4.3 Risk Level

The last step in preliminary risk estimation is to make one more classification: the risk level. There are five categories specified in the Standard. The Standard does not give guidance as to what hazard categories rise to a level that must be addressed, and which are low enough to be neglected. This bears on the question of a given project's tolerance for risk, which greatly varies between systems and industries.

Table 4-1: Risk Assessment Matrix per Previous Version of the Standard

Value	Risk Level
1 - 5	High
6 – 9	Serious
10 – 17	Medium
18 - 20	Low
21	Eliminated

In the past version of the Standard, a numerical value was assigned to each combination of severity and probability, yielding 20 possible "risk indexes" organized as 1 = highest risk, 20 = lowest risk. The new probability level "eliminated" is given a risk index of 21. This is still useful as intermediate step in preparing automated spreadsheets.

In the current version, the Standard includes a risk assessment matrix (table III) that formally combines severity and probability to yield a single risk level, which is reproduced below.

Table 4-2: Risk Assessment Matrix

Risk Assessment Matrix		Severity			
		Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Probability	Frequent (A)	High	High	Serious	Medium
	Probable (B)	High	High	Serious	Medium
	Occasional (C)	High	Serious	Medium	Low
	Remote (D)	Serious	Medium	Medium	Low
	Improbable (E)	Medium	Medium	Medium	Low
	Eliminated (F)	Eliminated			

5 Risk Mitigation

The last step in the hazard analysis is to consider mitigation and the recommended actions to address the hazards. Proposed actions are entered into the column labeled "Risk Mitigation" on the Hazard Analysis form. The standard establishes four broad categories of mitigation:

- Change the design or select design options that eliminate the hazard;
- Incorporate safety devices (railings, guards, safety controllers, etc.);
- Provide warning devices; and
- Develop procedures and training.

The LSST engineering team performing the hazard analysis uses this column to give a detailed description of the mitigation action.

5.1 Review and Acceptance of Residual Risk

LSST expects and attempts to reduce the mishap risks identified in the hazard analysis process to as low as possible and to an acceptable level of risk.

The risks remaining after all risk management measures have been implemented during the hazard analysis process are considered residual mishap risks. LSST recognizes and plans for interdependencies but approaches each risk class differently to allow an appropriate level of analysis and tracking. Hazards that have unresolved mitigations or continue to represent a risk to the project are referred to the Project Risk Register for high-level tracking; they are also kept in the Hazard Register for detailed handling.

For those risks that cannot be eliminated or controlled with engineering, the project will accept residual risks in the design at the levels of "Low" to "Medium" Mishap Risk Category depicted in Table 5-1. The project will work to further mitigate those risks through procedural methods or possible design modifications.

Table 5-1: Risk categories and mishap risk acceptance levels

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	AURA/SLAC/ NSF/DOE*
6 – 9	Serious	LSST Director/LSST Deputy Director/Project Manager
10 – 17	Medium	Subsystem Manager
18 – 20	Low	Engineering Manager

* High values are generally not acceptable for the LSST Project.

"High" category risks must be elevated to AURA, SLAC, NSF, and DOE. "Serious" category risks must be elevated to the Project Director, Deputy Director, and Project Manager and accepted as a project-level risk. The Subsystem Manager is responsible for elevating and reporting these residual mishap risks through entry on the LSST Project Risk Register. The Project Manager may apply additional resources or other remedies to help resolve these hazards and mitigate them to a lower level. Those hazards that continue at the "Serious" or "High" level are then processed by the Project Manager. The Project Manager has the responsibility for documenting that the appropriate authorities have formally accepted the "Serious" or "High" residual risks classifications. The Project Manager, Safety Manager, Systems Engineering Manager, and Subsystem Manager will jointly monitor the status of these elevated hazards through the regular Risk Management Plan described in LPM-20.

As noted in Table 5-1, hazard items that continue at a "High" level are generally not accepted for the LSST Project. Any such items will be considered a significant priority for resources to mitigate through redesign. Further, in some cases, individual institutional terms and conditions specifically do not allow residual assessments in the "High" category and must be resolved to a lower level before proceeding further with the project. For "High" and "Serious" risks, the project shall provide a documented rational that explains why the project was unable to reduce the risk with a justification for accepting the "High" or "Serious" risk.

5.2 Tracking of Hazards and Residual Risk

5.2.1 Project and Major Subsystem Tracking

A tracking system for hazards, their closures, and residual mishap risk will be maintained throughout the LSST lifecycle in the LSST Hazard Analysis Registers (spreadsheet) and the Risk Register. Each major subsystem will have a current log of identified hazards and residual mishap risk, including an assessment of the residual mishap risk after assuming that specific mitigation strategies will be applied. As changes are integrated into the system, this log is updated to incorporate added or changed hazards and the

associated residual mishap risk. The project will formally acknowledge acceptance of system hazards and residual mishap risk as referenced in the previous section. Users will be kept informed of hazards and residual mishap risk associated with their systems. The Project Manager is responsible for ensuring the maintenance of the LSST Hazard Risk Register of all identified project risks and "Serious" and "High" residual mishap risks identified in the Hazard Analysis process. The major Subsystem Manager or Subsystem Systems Engineer will communicate known hazards and associated risks of the system to all system design build contactors, subsystem engineers, and users.

5.2.2 Design Build Contractors

Design-build contractors are responsible for communicating information to the Subsystem Manager or Subsystem Systems Engineer on system hazards and residual mishap risks, including any unusual consequences and costs associated with hazard mitigation. After attempting to eliminate or mitigate system hazards, the design-build contactor shall formally document the hazards for tracking and notify the project of all hazards and with special attention to those that reach the "Serious" to "High" mishap risk categories. The following is an overview of the process:

1) The contractor performs an initial Hazard Analysis, guided by the LSST Hazard Analysis Plan LPM-49 and the Subsystem Hazard Analysis reference design spreadsheet.
2) The contractor completes and updates the system Hazard Analysis at each stage and identifies a mitigation strategy that brings the residual risk down as much as possible.
3) The LSST Project reviews, then rejects or accepts the Hazard Analysis mitigation plan, including the level of residual risk during each of the system acquisition phases.
4) The Subsystem Systems Engineer tracks all hazards to verify that the mitigation proposed and accepted by the project is actually implemented, and that it is tested and verified.
5) As changes are integrated into the system, the project will update the LSST Hazard Analysis Register (spreadsheet) to incorporate added or changed hazards and the residual mishap risk identified.

Throughout the LSST project life, the Project Manager will ensure that new hazards are evaluated and the resulting residual mishap risk either recommends further action to mitigate the hazards or formally documents the acceptance of these hazards and residual mishap risk. The Project will evaluate the hazards and associated residual mishap risk in close consultation and coordination with the ultimate end user, to assure that the context of the user requirements, potential mission capability, and the operational environment are adequately addressed.

Copies of the documentation of the hazard and risk acceptance will be provided to both the design-build contactor and the system user. Hazards for which the Project Manager accepts mitigation responsibility will also be included in the formal documentation. Residual mishap risk and hazards must be communicated to system test efforts for verification.

6 Analysis Process

6.1 Hazard Analysis Meetings

The primary means for making progress with the hazard analysis during the design phase is based on a regular assessment meeting. Each meeting is dedicated to a specific area, subsystem or process. The meeting length varies but last for approximately one hour. This length has been found to be productive and suitable for maintaining focus and avoiding distractions.

6.2 Field Inspections

The primary means for making progress with the hazard analysis during the construction phase and subsequent phases is based on regular field inspections and assessment meetings. Additional feedback from experience in the field will be included in the hazard analysis process.

6.3 Project Risk Assessment

The hazard analysis process is considered a subsystem of the overall project risk assessment. Therefore, any identified hazard not mitigated through this hazard analysis process is to be included in the overall project risk assessment.

6.4 Personnel Roles

The number of attendees in Hazard Analysis meetings will vary depending on the topic. The minimum shall be the responsible system engineer for the major subsystem, or a designated alternate to guide the process; the lead engineer or engineers with particular focus on covering appropriate disciplines (architecture, mechanical, electrical, software etc); An electrical/controls engineer to represent the LSST Safety Interlock System, and the safety engineer overseeing the subsystem.

6.4.1 Systems Engineer

The systems engineer for the major subsystem under review shall take the lead role in hazard analysis, organizing the topics and the meetings. Their responsibility includes

- Scheduling hazard analysis meetings;
- Determining attendees;
- Presiding over and serving as facilitator during the meetings;
- Filling in the columns of the of the hazard analysis form as work proceeds;
- Terminating the meeting at the appropriate time;
- Reporting progress to non-attendees via the project's weekly reports; and
- Maintaining the subsystem Hazard Analysis Register.

6.4.2 Lead Engineer

The lead engineer represents the hardware or process design (typically brings drawings or other design

documentation) of the assembly under analysis and takes the lead in walking through the subsystems. It is essential that some sort of systematic approach be taken to the problem so that important elements are not forgotten or neglected.

The lead engineer also has the best understanding of anticipated activities during all relevant phases of work on the assemblies. It is useful, in architectural parlance, to "get small" and imagine working with and/or around the equipment in question.

6.4.3 Electronics/Controls Engineer

An electronics/controls engineer is present at all meetings to represent the Safety Interlock System (SIS). This participant contributes an understanding of the capabilities of the SIS and reports back on enhanced requirements and functions for the system.

6.4.4 Safety Engineer

The safety engineer or designated safety professional, at the institution with the lead responsibility for the subsystem under analysis participates in these meetings to insure compliance with the LSST Safety Policy, local Safety, Health and Environment plans and to provide general guidance on hazard safety issues.

7 Documentation

The system engineers, or duly appointed alternate, within each major LSST subsystem, Data Management, Telescope and site, Camera, Systems Engineering, shall maintain a single Hazard Analysis Register with a minimum of the entries provided in Appendix A. This sheet shall be updated periodically and posted in the Collection-3607 of the LSST archive for broad access and review.

8 Bibliography

- Department Of Defense. *Standard Practice for System Safety.* MIL-STD-882D, 10 February 2000.
- Department Of Defense. *Standard Practice for System Safety. Environment, Safety, and Occupational Health Risk Management Methodology for Systems Engineering.* MIL-STD-882D w/CHANGE 1. Draft Dated 29 March 2010.
- Ericson, Clifton A. II. *Hazard Analysis Techniques for System Safety.* Hoboken, New Jersey: John Wiley and Sons, 2005.
- ATST Project, Rob Hubbard, Hazard Analysis Plan, SPEC 061.

Appendix A – LSST Hazard Analysis Form

ITEM ID	MACHINE OR SUB-PROCESS	USER	TASK DESCRIPTION	HAZARD CATEGORY	HAZARD	CAUSE OR FAILURE MODE	PROJECT PHASE	Prior to Safeguard Selection				RISK MITIGATION
								SEVERITY	PROBABILITY	RISK INDEX	RISK LEVEL	
								Four Levels	Six Levels	1 to 21	Five Levels	
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												