Large Synoptic Survey Telescope Camera System Plan	Document # **LCA-31-B**		Status LSST Camera APPROVED Effective Date: 9 Sept 2014
	Author(s) Martin Nordby Nadine Kurita	Frank O'Neill	
	Subsystem/Office Performance and Safety Assurance		

Document Title

LSST Camera System Safety Program Plan

1. Change History Log

Revision	Effective Date	Description of Changes
A	13 Oct 2011	Initial release. See notice LCN-001.
B	9 Sept 2014	General update in preparation for CD-2 review. See LCN-1111. Revised the Risk Acceptance Matrix, removed the System Hazard Analysis as these system hazards are included in the HAR, added probability ranges as a guide to the probability definitions, updated the System Safety Analysis and Documentation Flow figure.

2. Contents

3. Acronyms and Definitions

3.1. Acronyms

ALARP	as low as reasonably practicable
CD-n	Critical Decision
CoDR	Conceptual Design Review
CPM	Camera Project Manager
CPS	Camera Protection System
ES&H	Environment, Safety, and Health
ESF	Engineered Safety Feature
FDR	Final Design Review
HAR	Hazard Analysis Report
I&T	Integration and Test
LSST	Large Synoptic Survey Telescope
LSSTC	Large Synoptic Survey Telescope Corporation
O&SHA	Operating and Support Hazard Analysis
OCD	Operations Concept Document
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PMP	Project Management Plan
PPA	Particle and Particle-Astrophysics
PPE	Personnel Protective Equipment
PSA	Performance and Safety Assurance
PSAP	Performance and Safety Assurance Plan
SEMP	System Engineering Management Plan
SIM	Systems Integration Manager
SLAC	Stanford Linear Accelerator Center
SSE	System Safety Engineer
SSP	System Safety Program
SSPP	System Safety Program Plan

SSWG System Safety Working Group

3.2. Definitions

Acceptable Risk: that level of residual safety risk that the managing authority is willing to assume on behalf of the agency, users and public

As low as reasonably practicable (ALARP): that level of risk which can be further lowered only by an increment in resource expenditure that cannot be justified by the resulting decrement in risk

Hazard: potential for harm; also, a condition prerequisite to a mishap

Interim Risk: the risk that is present until final mitigation actions have been completed

Mishap: accident; an unplanned event or series of events resulting in death, injury, system damage, loss of or damage to equipment of property, or insult to the environment

Residual Mishap Risk: the mishap risk that remains after all approved mitigators have been implemented and verifier

Risk (also referred to as mishap risk): a measure of the expected loss from a given hazard or group of hazards; risk is a combined expression of loss severity and probability or likelihood

System Safety: the application of engineering and management principles, criteria, and techniques to achieve mishap risk as low as reasonably practicable (to an acceptable level), within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system lifecycle

Test: identifies an in-process test or measurement, which can include a dimensional measurement, electrical continuity or functional test, or a more complete performance verification test.

4. Applicable Documents

[1] ANSI/GEIA-STD-0010-2009, “Standard Best Practices for System Safety Program Development and Execution”

[2] LCA-10090, “SLAC Institutional Safety Implementation Plan”

[3] LCA-15, “LSST Camera Hazard List.”

[4] LCA-226, “LSST Camera Project Management Plan,”

[5] LCA-138, “Camera Performance and Safety Assurance Plan,”

[6] LCA-38, “LSST Camera System Engineering Management Plan”

[7] SLAC-I-720-70100-100, SLAC Environment, Safety, and Health Manual

[8] LPM-18, LSST Safety Policy

[9] LCA-14, “LSST Camera Hazard Analysis Report

[10] LCA-282, “Camera Operations Concept Document”

[11] LCA-40, “Camera Integration and Test Plan”

5. Purpose and Scope

The LSST Camera System Safety Program Plan (SSPP) describes the tasks and activities associated with the Camera System Safety Program (SSP), which has the purpose of identifying the hazards of the Camera and imposing design requirements and management controls to prevent mishaps and mitigate their impact. This SSPP also defines the goals and requirements of the System Safety effort and establishes the framework within which these goals are satisfied and the requirements most efficiently and effectively fulfilled. The focus of the SSP is the design and operation of the Large Synoptic Survey Telescope (LSST) Camera. The SSP covers all phases of the program including design, development, fabrication, assembly, handling, transportation, storage, integration, test, and operation. The objective of the SSPP is to define a systematic approach that ensures the following:

Safety is optimized in the design, construction, and operation of the Camera, consistent with performance, schedule and budget

Hazards associated with the system are identified and evaluated for all phases of the program.

The risks associated with all identified hazards are controlled to acceptable levels.

New hazards are not introduced into the system through design changes.

Requirements for retrofit actions necessary to eliminate or control hazards are minimized.

The policy of management is to design for minimum risk.

The camera project team is composed of collaborating institutions within the United States and in France, and is a subsystem of the LSST Observatory, which is managed by the LSST project in Tucson, Arizona. The Camera System Safety Program Plan supports and is subordinate to [Ref 4], the Camera Project Management Plan (PMP) and [Ref 5], the Performance and Safety Assurance Plan (PSAP). Furthermore, the Camera SSP is responsive to the LSST Safety Policy [Ref. 8] and the LSST Observatory System Safety Plan requirements.

The SLAC Institutional Safety Implementation Plan [Ref. 2]addresses site-specific safety processes and plans associated with general occupational safety issues including visitor access, work planning and control, emergency procedures, training, and other institutional ES&H safety matters. These topics are the purview of [Ref 2] and are explicitly not within the scope of this Plan.

[Ref 6], the LSST Camera System Engineering Management Plan (SEMP), addresses risks associated with meeting camera performance requirements. [Ref 6] specifically does not address risks associated with hazards, while this SSPP only includes system safety risks and not those pertaining to failure to meet performance requirements.

[Ref. 9], the Camera Hazard Analysis Report describes camera functionality and documents camera hazards identified using the process described in this Plan, as well as plans for mitigating them.

6. System Safety Program Management

6.1. Camera Organization and Management

The LSST camera team consists of members from geographically diverse organizations and is managed by the Camera project officeat the SLAC National Accelerator Lab (SLAC). The Camera System organizational structure is shown in Figure 1. The Camera Project Director provides overall project direction, while the Camera Project Manager (CPM) has responsibility for day to day execution of the project. The CPM is supported by the Camera Systems IntegrationManager (SIM) and Performance and Safety Assurance (PSA)group in the execution, technical oversight and coordination of the Camera development, construction and commissioning activities. Camera Subsystem Managers report to the project manager, with the SIM and PSAgroup providing technical support and oversight.

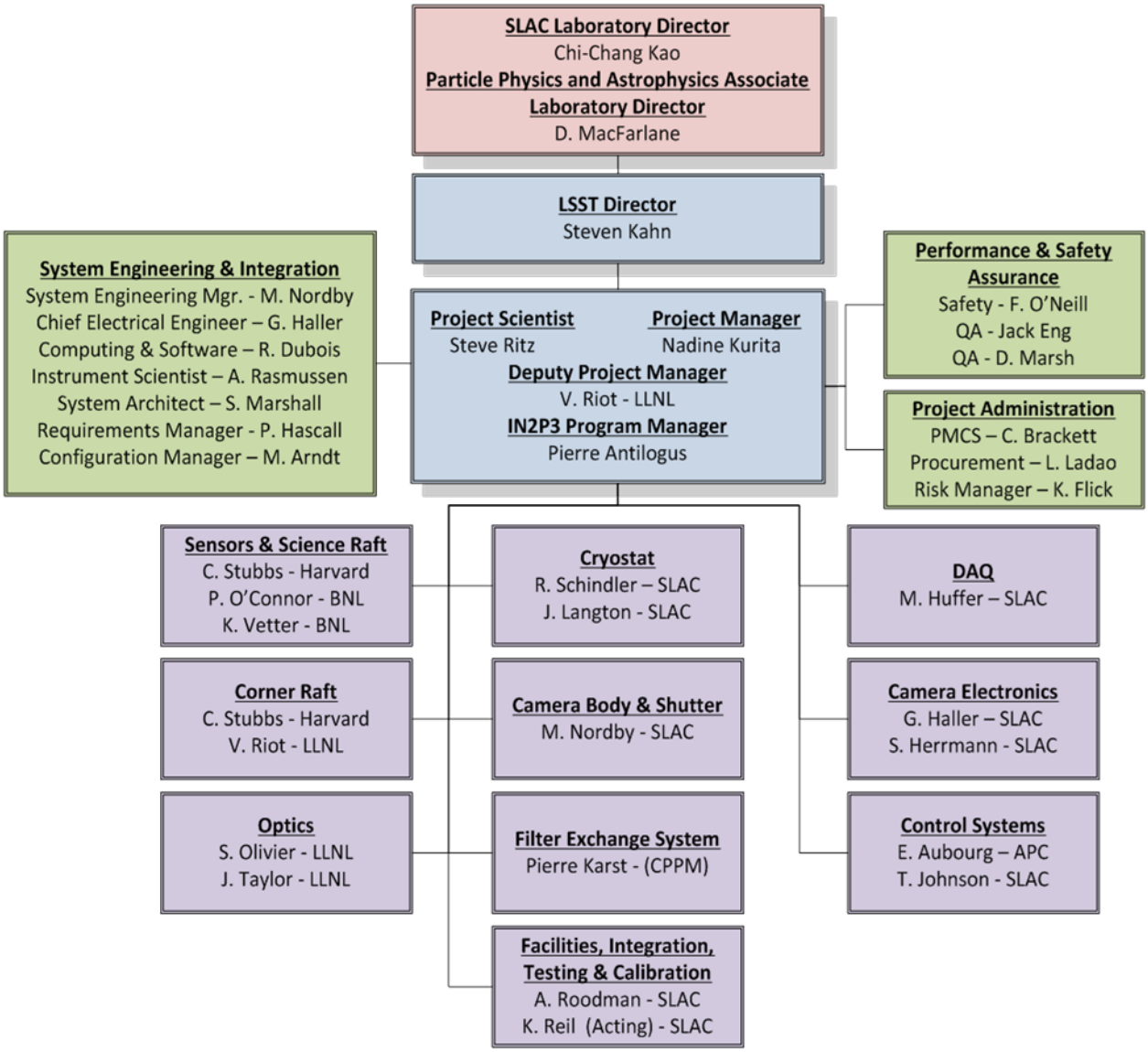

Figure 1: Camera Project Organization

The Camera is one of three subsystems of the LSST Observatory. As such, the CPM reports to the LSST Project Office . Management and system safety processes formally flow down along this channel. However, the Camera management works closely with counterparts in the LSST organization to ensure that the Camera SSP integrates closely with the Observatory SSP.

6.2. System Safety Program Organization, Management, and Responsibilities

6.2.1. Organization

The CPM has assigned a System Safety Engineer (SSE) to establish and implement the SSP. The SSE is organizationally located in the Performance and Safety Assurance group, and the SSE has direct access to the CPM to report on safety issues and make recommendations to resolve them. In addition, the Camera SSE reports directly to the Director of the Particle and Particle-Astrophysics (PPA) directorate at SLAC and is therefore able to raise safety issues directly to the attention of top management of SLAC, if necessary.

The System Safety Program is integrated with the overall project management of the Camera, with the SSE providing a focal point for safety activities. As such, responsibilities for managing the SSP fall along the line management of the project. Roles and responsibilities for implementing the SSP are as follows:

6.2.2. Camera Project Manager Roles and Responsibilities

The CPM has the overall responsibility for ensuring that system safety is incorporated into the Camera project at all levels. The CPM implements the safety policy and objectives by

Ensuring that the SSP is established and integrated throughout the Camera project.

Ensuring that hazards are identified and risk is eliminated or controlled within acceptable limits.

Ensuring that Camera design and operations meet applicable safety standards, as detailed in Section 4, above and safety regulations as called out in [Ref 5].

Reviewing and approving safety analyses and documents submitted to either the LSST project or sponsoring institutions.

6.2.3. System Safety Engineer Roles and Responsibilities

The SSE is the focal point for all safety activities involved in implementing the Camera SSP. The SSE influences the design when necessary in the interest of safety, and with the goal of minimizing the overall hazard level of the camera design and operations. This requires that the SSE is actively involved in many aspects of the project. The SSE is responsible for:

Participating as a member of the LSST Safety Council

Participating in design reviews

Preparing the SSP deliverable documents

Supporting the LSST SSP implementation and providing the primary interface to the Camera

Developing and establishing safety design criteria and safety design requirements as needed

Reviewing and approving selected drawings, specifications, and procedures

Participating in hazardous testing and system safety testing

Evaluating design changes for their impact on safety

6.2.4. Camera Subsystem Managers Roles and Responsibilities

Camera Subsystem Managers or their designee are responsible for integrating safety into their subsystem and supporting the Camera SSP. Identified members of each subsystem directly support the SSP activities, and receive technical assistance from the SSE for resolution of safety issues involving the Camera and its subsystems.

6.2.5. LSST Camera System Safety Working Group

The System Safety Working Group (SSWG) consists of representatives from each subsystem. The SSWG meets at appropriate intervals and collaboration meetings. The purpose of the SSWG is to assist LSST Management in achieving the system safety objectives.

6.3. System Safety Program Review

Periodic reviews of the LSST Camera System Safety Program are conducted with representatives of the LSST project participating.

7. System Safety Program Methodology

7.1. Overview

System Safety applies engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness, schedule, and cost, throughout all phases of the system lifecycle. As shown in Figure 2, SSP requirements are grouped into five major elements: Program Initiation, Hazard Identification, Risk Assessment, Risk Reduction, and, Risk Acceptance. These five elements are introduced in the following sections and detailed starting in Section 9. Figure 2 also illustrates that System Safety is an iterative process that requires continuous involvement of safety personnel to remain informed of the design as it evolves and matures in order to evaluate the impact of any change on hazards and/or their associated controls.

7.2. Program Initiation

LSST CPM approval and release of the SSPP document is the initial step in launching the System Safety Program. The SSPP identifies the system safety organization, tasks, activities, responsibilities, and the approach to managing risk. The plan also outlines the planned approach for safety task accomplishment.

7.3. Hazard Identification and Tracking

Complete identification of all hazards associated with camera systems and tracking of these hazards through the lifecycle of the program is essential to meeting the goal of the SSP. In general this is accomplished by identifying the source-mechanism-outcome of each hazard. See Section 8 for a description of the hazard analysis tasks, and Section 9, for a description of the hazard analysis process.

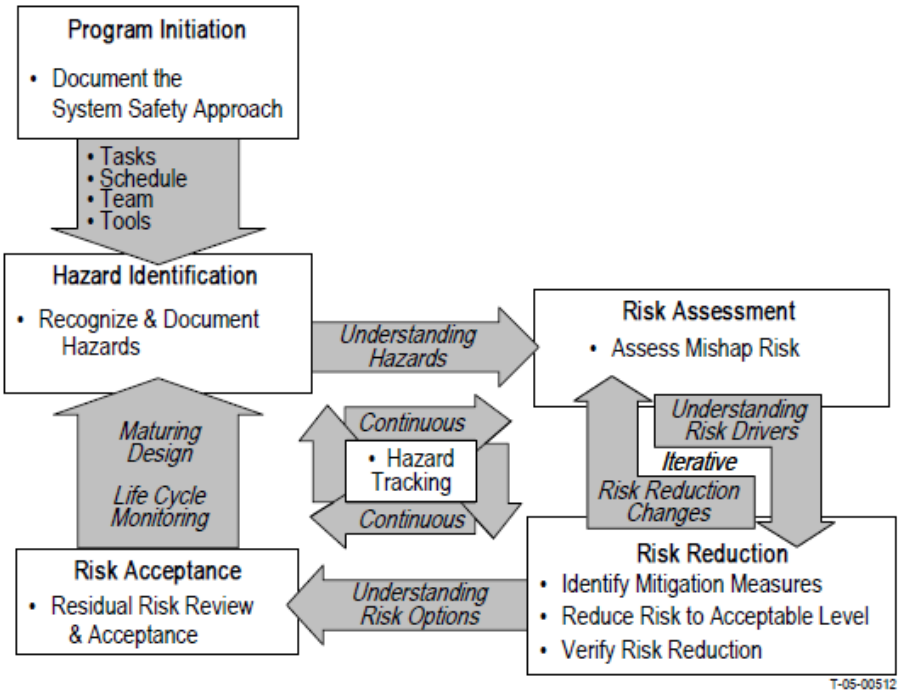

Figure 2: Safety Program Elements and Flow

7.4. Risk Assessment

For each identified hazard, the mishap severity and probability or frequency are established. As detailed in Section 9, a mishap risk assessment matrix is used to assess and display the risks. The risk assessment is a subjective judgment based on history and system knowledge.

7.5. Risk Reduction

Risk reduction is achieved by accomplishing the following steps. a) understand the risk drivers; b) develop and document candidate mitigators; c) select and implement mitigators in accordance with the system safety mitigation order of precedence; d) verify that the risk has been reduced. The system safety order of precedence is detailed in Section 9.

7.6. Risk Acceptance

Under advisement of the SSWG, the CPM makes decisions regarding the acceptability of residual mishap risk and the cost of risk mitigation measures. Decisions and decision-making authority are classified by the risk acceptance level of a hazard. There are four levels of risk acceptance, graded by the severity of the hazard. These are:

High: generally not acceptable to the camera project, AURA, NSF, SLAC, and the DOE; all would have to accept this level of risk

Serious: undesirable; requires a decision by LSST Project Director, Deputy Director, LSST Project Manager, and Camera Project Manager

Medium: acceptable with review by the Camera Project Manager

Low: acceptable with review by the Camera Subsystem Manager

8. Program Deliverables

8.1. Camera System Safety Tasks

The Camera system safety program is centered around the progressive analysis of hazards associated with the Camera system design and operation plans. This starts at the conceptual design phase and proceeds through preliminary and final design of camera subsystems, development of operations plans and procedures, and continues through delivery, commissioning, operations, and any upgrades. The documents resulting from this analysis are described below, with their contents outlined in the following sections:

System Safety Program Plan (SSPP): this document; describes the plan for implementing the system safety program for the camera project.

Hazard Analysis Report (HAR) [Ref. 9]: identifies safety-critical areas and provides an assessment of hazards and requisite mitigations and follow-on actions. This begins as a Preliminary Hazard Analysis (PHA), then is revised as hazard assessments are refined consistent with the preliminary and final designs of camera elements.

Operating and Support Hazard Analysis (O&SHA): evaluates hazards introduced into the system by activities associated with operations and support procedures, and evaluates the adequacy of the procedures to eliminate, control, or abate the hazards.

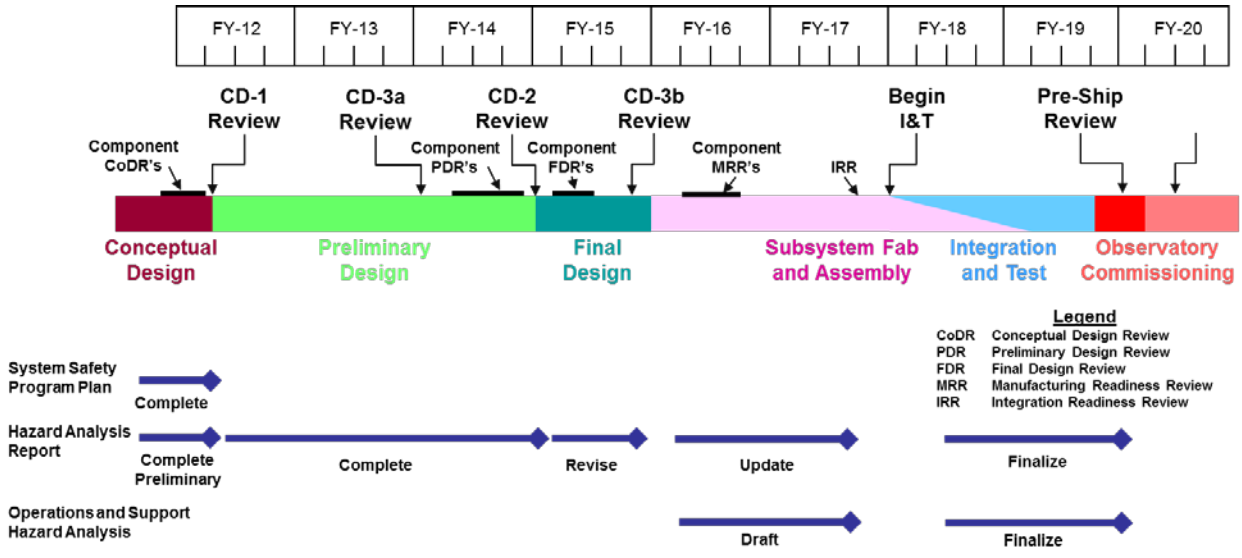

Figure 3: System Safety Analysis and Documentation Flow

Figure 3 shows a flow chart of the analysis tasks and resulting document deliveries, along with camera project milestones.

8.2. Documentation Details

8.2.1. Hazard Analysis Report

8.2.1.1. Purpose and Contents

The HAR identifies safety-critical areas and provides an assessment of hazards and requisite mitigation, controls and follow-on actions. A functional and physical description of the hardware is included, as well as a description of the hazards and mitigation plans. Hazards associated with the proposed design or function are evaluated for hazard severity, hazard probability, and operational constraints, based on the best available data including mishap data from similar systems and other lessons learned. Mitigation plans and verification methods to reduce the hazard and associated risk are included.

The HAR considers the following for identification and evaluation of hazards:

Hazardous components: toxic substances and materials, pressure systems or other systems involving stored energy.

Interfaces: interfaces involving safety considerations, including material compatibility, electromagnetic interference, inadvertent activation, fire initiation and propagation, and hardware and software controls.

Design criteria: criteria for safety-critical software commands and responses to failures such as inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or other designated undesired events.

Environmental constraints: including potentially hazardous operating environments such as shock, vibration, extreme temperatures, humidity, noise, working at elevation, hypoxia, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, ionizing and non-ionizing radiation including laser radiation.

Human factors engineering: mishaps due to operator error during operation, test, maintenance, or emergency response. This includes assessment of the effect of factors such as equipment layout, lighting, and ergonomics.

Test-unique hazards: hazards associated with, or a direct result of, test or evaluation of a component or system.

Facilities and support equipment: hazards introduced by handling and test equipment, or existing in the facility being used by camera hardware; maintenance of hazardous and safety-critical systems.

Training and certification: required training pertaining to hazardous and safety-critical operations and as mitigation of hazardous conditions.

Safety-related equipment: safeguards, interlocks, redundancy, fail-safe design considerations, hardware or software controls and protection systems, fire detection and suppression systems, personnel protective equipment.

[Ref. 3], the Camera Hazard List is developed to delineate and track all hazards identified in the HAR. The Hazard List includes the following: subsystem, hazard type, hazard description, unmitigated risk, summary description of hazard controls, risk assessment with controls in place, verification method/s, Camera Protection System (CPS) requirement, and subsystems associated with interface hazards. This is used for managing the hazards and development of appropriate mitigation plans. The Hazard List delineates hazards with suitable detail to allow for tracking the development of the mitigation over the life of the design development, to ensure that the mitigation is appropriately incorporated into the design and operations plans, and that it is reviewed and implemented in the final design of the system. This is

intended to be a living document that is reviewed and updated on a regular basis, thus providing Camera management and system engineering organizations a tool for actively addressing and tracking identified hazards.

Hazard Reports are developed for hazards that may have a significant impact and/or require more detailed documentation to describe hazards and the mitigation measures. In particular, hazards that rank high on the Hazard List are flagged by the SSE and Hazard Reports are generated to provide additional detail as to the complexity or severity of the hazard or the details of the mitigation. Hazard Reports are also used where hazards are suitably complex or interrelated that their mitigation goes beyond a single subsystem or design element.

The HAR begins as the Preliminary Hazard Analysis (PHA) report, reflecting the less-than-complete understand of camera design and hazards associated with early-stage design development. This is then refined and hazards assessed consistent with the preliminary and ultimately final design stages of the camera. This includes updating the hazards to match the hardware and software design and to capture hazards associated with interfaces in their final incarnation. The HAR also documents the validation that requisite controls are incorporated into the final design and operations plans. Finally, this provides a description of the verification methods associated with verification of hazard mitigation measures. This includes analysis, quality assurance inspection and testing of components, as well as functional tests to verify performance of protection and safety devices and systems.

The Hazard List and Hazard Reports are similarly updated to and are delivered with the HAR.

8.2.1.2. Disposition and Close-Out

The initial PHA is drafted and submitted for review prior to the Camera Critical Decision 1 (CD-1) Review and Conceptual Design Review (CoDR).). The PHA is then revised and re-named the Hazard Analysis Report which is delivered prior to the CD-2 Review and updated again in the final design stage in preparation for the CD-3 Review.

Following the CD-3 Review but prior to first-test of subsystem hardware assemblies, the plan for the verification of all HAR hazard controls should be completed. The process of iteratively reexamining the impact of design changes on hazards and the effectiveness of mitigation methods continues up to delivery and afterward, if necessary.

8.2.2. Operating and Support Hazard Analysis

8.2.2.1. Purpose and Contents

The Operating and Support Hazard Analysis (O&SHA) evaluates hazards introduced into the system by activities associated with operations and support procedures, and evaluates the adequacy of the procedures to eliminate, control, or abate the hazards.

The O&SHA examines procedurally-controlled activities, identifying and evaluating hazards resulting from implementation of operations or tasks performed by persons. The following factors are considered in this evaluation:

Planned system configuration or state at each phase of activity

Facility interfaces

Planned environments and environmental ranges

Supporting tools and equipment, including software-controlled automatic test equipment

Operational or task sequence and limitations

Personnel safety and health requirements

Potential for unplanned events, including hazards introduced by human error

The evaluation also includes a functional and physical description of the support and test equipment and how it interfaces with human operators.

The O&SHA identifies safety requirements or alternatives needed to eliminate or control identified hazards or to reduce the associated risk to an acceptable level. The analysis addresses the following:

System states: potentially hazardous system states that are under operator control.

Activities that occur under hazardous conditions: time periods and actions required to minimize risk during these activities and time periods.

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

Safety devices: requirements needed for safety devices and equipment, including personnel safety and life support equipment.

Required emergency procedures: warnings, cautions, and special procedures to prepare for egress, escape, or rescue, in the event of a system failure.

Hazardous materials handling: requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous material.

Training: requirements for training and certification of personnel.

8.2.2.2. Disposition and Close-Out

The O&SHA is developed in conjunction with finalizing [Ref. 10], the Operations Concept Document (OCD) and [Ref. 11], the Integration and Test (I&T) Plan. The O&SHA complements the development of operational and support procedures and is delivered as part of the documentation for final delivery of the Camera.

9. Hazard Analysis Process

9.1. Hazard Analysis Process Overview

The hazard analysis process outlined below is also provided again in each of the Hazard Analysis documents in order to allow these documents to stand alone. The process serves as the primary means for understanding and managing risks associated with the design and operation of the LSST Camera. This is an eight-step process that is outlined below and detailed in the subsections that follow.

Define Camera System Characteristics: define the physical and functional characteristics of the camera systems utilizing design documents, specifications, drawings, and technical reports, as necessary

Identify Camera Hazards: list hazards related to all aspects of the camera project that pose a risk of personnel injury, system safety, or environmental damage and determine their causes

Assess Hazard Severity Class: classify each hazard by the potential degree of harm that could result from a mishap

Define Hazard Probability Level: estimate the likelihood of a mishap occurring

Assign a Risk Assessment Value and Category: this is a number 1-20, based on the Severity Class and Probability Level

Implement a Risk Reduction/Mitigation Strategy: choose a strategy for reducing the Risk Assessment Value, if needed and act on it

Re-assess: repeat the process using the newly-mitigated hazard and iterate until the Risk Value is deemed to be reduced to an acceptable level

Identify a verification method: identify and describe the means by which the mitigation activities will be verified to have been implemented

This analysis process is qualitative, in that it is based on engineering judgment and weighing of relative risk. The result is a prioritized Hazard List, showing all identified hazards along with mitigation and verification plans. Hazard Reports are also developed for hazards that may have a significant impact or require more detailed documentation to describe hazards and the mitigation measures. The process is derived from [Ref 1], ANSI/GEIA-STD-0010-2009, “Standard Best Practices for System Safety Program Development and Execution.”

9.2. System Characteristics Definition

A detailed physical and functional description of each camera subsystem is necessary to allow a technically competent person to review the hazard analysis documentation and understand the pertinent issues. The level of detail should be sufficient to allow an adequate characterization of the systems, the associated hazards and their potential impact.

9.3. Hazard Identification

A hazard is any real or potential condition that can cause injury, illness, or death to personnel, damage to or loss of a camera subsystem, damage to equipment or property; or damage to the environment. For the

LSST Camera and most engineered systems, hazards are often associated with the unplanned failure of a component, inadvertent misuse, non-standard operations, or the interjection of unforeseen outside influences including other hardware or systems, personnel, or environmental forces. The first step in the hazard assessment process is the identification of all hazardous situations. Hazards are organized into the types listed below, delineating the energy source or agent for initiation of a mishap. This is used both to aid in identifying hazards and for use in managing them.

Thermal: overheating, extreme cold, excessive rates of change, thermal-mechanical stressing

Pressure/Vacuum: over-/under-pressure, rupture/collapse

Mechanical: collision, dropping, loss of function, mechanical failure, pinching

Structural: collapse or failure, deformation or buckling, sensitivities to vibration/shock/noise including seismic activity

Electrical: over-/under-current, short to ground, electro-static discharge

Control: loss of control, unexpected shut-down/start-up, loss of interlocks, loss of redundancy, operator error

Environmental: humidity, oxygen deficiency

Fire: vapors and chemical reactions, effects of excessive heat

Materials and substances: spill, release of, or exposure to materials which can damage equipment, cause environmental harm, pose health or safety risks to personnel; this includes contamination due to material release

Contamination: damage to equipment due to unplanned exposure to contaminants

For each hazard type listed, hazards are identified that pose a risk to hardware, personnel, or the environment from these sources or that the hardware poses to other hardware, personnel, or the environment. This is for all phases of assembly, integration and test, operations, and servicing and should also reference any safety risks due to hazards that cross interfaces.

Hazards should be identified for all credible situations associated with Camera hardware. Where “credible” is defined as a situation that could plausibly occur, even if the likelihood is remote. Thus, a structural failure due to a large earthquake would be considered a credible hazard, while structural failure due to an asteroid impact would be considered non-credible.

Furthermore, hazards should be identified in association with a particular component or item, with an emphasis on specificity. This is important to ensure that the mitigation strategy and verification methods relate to the identifiable process and not just generalities. For example, a hazard of “structural failure” is not nearly specific enough to be associated with verifiable mitigation, but “structural failure of a lens mounting flexure” is adequately specific to allow for verifiable mitigation steps.

Finally, hazards are associated with the consequences of an accident or incident coming to pass. Thus, the potential failure of a component may produce more than one type of consequence, where consequence type is associated with personnel injury, system damage, or environmental damage. All types of consequences must be listed, but this is identified as a single hazard.

9.4. Hazard Severity Classes

Severity is an assessment of the worst potential consequence which could occur from a hazard coming to pass. Four categories of hazard severity are defined:

Class 1: Catastrophic
Class 2: Critical
Class 3: Marginal
Class 4: Negligible

See Table 1 for a definition of each severity class, specified by degree of injury, level of property damage, or impact on the environment if the identified hazard resulted in an accident.

Table 1: Hazard Severity Classification

Class	Description	Potential Consequences
1	Catastrophic	Injury: may cause death or permanently-disabling injury Property damage: near-complete loss of camera system Environment: irreversible severe environmental damage
2	Critical	Injury: severe injury, occupational illness, or permanent partial disability Property damage: major damage to system; loss of major subsystem(s) Environment: significant reversible environmental damage
3	Marginal	Injury: minor injury or occupational illness Property damage: minor damage to camera or subsystem, recoverable with minimal impact on program Environment: mitigatible environmental damage, where restoration activities can be accomplished
4	Negligible	Injury: minor first aid treatment; personal health not affected Property damage: systems or components experience more than normal wear and tear; easily recoverable within scope of standard maintenance Environment: minimal environmental damage

9.5. Hazard Probability Levels

Probability is the likelihood that an identified hazard will result in an accident or mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and the number of items posing the hazard. The specific range of values depicted is provided as a guide. Five levels of probability are defined:

Level A: Frequent
Level B: Probable
Level C: Possible
Level D: Remote
Level E: Improbable

See Table 2 for a definition of these probability levels.Table 2: Hazard Probability Levels

Level	Frequency of Occurrence	Definition
A	Frequent	Likely to occur often in the life of the Camera. ($X > 10^{-1}$)
B	Probable	Will occur several times in the life of the Camera. ($10^{-1} \geq X > 10^{-2}$)
C	Possible	Likely to occur sometime in the life of the Camera. ($10^{-2} > X > 10^{-3}$)
D	Remote	Unlikely but possible to occur in the life of the Camera. ($10^{-3} > X > 10^{-6}$)
E	Improbable	So unlikely, it can be assumed occurrence may not be experienced

9.6. Mishap Risk Assessment

The Risk Assessment Value is a numerical expression of comparative risk determined by an evaluation of both the potential severity of a mishap and the probability of its occurrence. It is a number from 1 to 20, assigned from the Mishap Risk Assessment Matrix shown in Table 3 . The Risk Assessment Value is used to prioritize hazards for risk mitigation actions and to group hazards into risk categories, as detailed in Table 4.

Table 3: Mishap Risk Assessment Matrix

		Severity			
		1—Catastrophic	2—Critical	3—Marginal	4—Negligible
Probability	A—Frequent	1	3	7	13
	B—Probable	2	5	9	16
	C—Possible	4	6	11	18
	D—Remote	8	10	14	19
	E—Improbable	12	15	17	20

Table 4: Mishap Risk Categories

Risk Assessment Value	Mishap Risk Category	Acceptance Criteria
1-5	High	AURA/NSF/SLAC/DOE[1]
6-9	Serious	LSST Project Director/Deputy Director/LSST Project Manager/Camera Project Manager [2]
10-17	Medium	Camera Project Manager
18-20	Low	Camera Subsystem Manager

[1] High values are generally not acceptable for the Camera project

[2] For the Camera project, the decision will be coordinated with the DOE Federal Project Director

9.7. Risk Reduction/Mitigation

The next step in the hazard analysis process is development of a risk reduction or mitigation process. There are six mitigation strategies that can be implemented to decrease the risk to an acceptable level within the constraints of time, cost, and system effectiveness. Resolution strategies in descending order of precedence are listed in the sub-sections below, and the extent and nature of how these strategies are implemented must be balanced against the other constraints on the system. For some hazards, more than one mitigation process may be used. However, the lowest-order mitigation method defines the "weakest link" and should be used for identifying the mitigation strategy in the Hazard List.

9.7.1. Eliminate Hazard Through Design Selection

The risk of a hazard can often be eliminated by selecting a design alternative that removes the hazard altogether. The hazard source or the hazardous operation is eliminated by design without degrading the performance of the system. Examples: using pneumatic rather than electrical actuators in an explosive atmosphere, selecting non-flammable hydraulic fluid, and replacing toxic with benign materials.

9.7.2. Control Hazard Through Design Alteration

If the risk of a hazard cannot be eliminated by adopting an alternative design, changes to the design or manufacturing plans should be considered that reduce the severity or the probability of a harmful outcome, thereby controlling the impact of the hazard. The major safety goal during the design process is to include features that are inherently safe, fail-safe, or have capabilities to handle contingencies through redundancy of critical elements or design conservatism. Complex features that could increase the likelihood of hazard occurrence should be avoided wherever feasible. System safety analysis should identify hazard control, damage control, containment, and isolation procedures. Examples of hazard control through design alterations include: using larger factors of safety on critical parts, adding redundancy, incorporating industry design or manufacturing standards.

9.7.3. Incorporate Engineered Safety Feature

If unable to eliminate or adequately mitigate the hazard through design, reduce mishap risk by adding protective Engineered Safety Features (ESF) to the system. In general, safety features are features added to the design with the specific purpose of providing static intervention and do not require active testing, monitoring, or control. Examples include: physical barriers, guards, end-of-travel stops, or fuses.

Note that safety features incorporated as part of the system, such as physical guards or barricades, should be distinguished from those requiring personnel use, such as hearing protection, lock-out device, add-on stops or limiters, or other items of personal protective equipment (PPE). Use of installed controls is generally preferable and more consistent with the system safety order of precedence. Additionally, the training component of protective equipment use needs to be considered as a procedure and training element that requires more ongoing resource commitment and is subject to more variables than safety devices intrinsic to the system.

9.7.4. Incorporate Safety Devices

If unable to eliminate or adequately mitigate the risk of a hazard through a design alteration or addition of ESF's, reduce the risk of a mishap coming to pass by using a safety device that actively interrupts the mishap sequence. Examples include: pressure-relief valves, loss-of-tension braking for elevators, fulltime on-line redundant paths, interlocks, ground-fault circuit interrupters, limit switches, shut-off switches or sensors and shut-off controls.

9.7.5. Provide Warning Devices

If design selection, ESF's, or safety devices do not adequately mitigate the risk of a hazard, include a detection and warning system to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event. This may include monitoring parameters such as voltages and currents, which can detect some incipient failures or trends which may lead to failures.

9.7.6. Develop Procedures and Training

Where other risk reduction methods cannot adequately mitigate the risk from a hazard, incorporate special procedures and training. Procedures may prescribe the use of PPE. For hazards that could result in mishaps, avoid using warning, caution, or written advisories or signage as the only risk reduction method. Examples of the use of procedures and training include: use of required PPE such as safety eyewear and hearing protection; procedures invoking the use of dedicated fixtures, added protection, or emergency shut-off devices.

9.8. Re-Assessment

As part of developing a mitigation strategy and mitigation plans, the hazard is re-assessed and a new Risk Assessment Value is determined. This new value is the risk level for the hazard with the mitigation in place. The goal is that the mitigation plans reduce the risk to a level low enough to be acceptable. This is an iterative process, and may require multiple levels of mitigation to reduce the risk. However, the outcome of the re-assessment is a new risk value that is deemed acceptable.

The impact of changes to the design as it matures and evolves also requires careful reevaluation of the hazards and the effectiveness of mitigation methods. This is a continuous process as the design progresses and is tracked in the hazard list.

9.9. Verification Method

Identify and describe the means by which the mitigation activities are verified to have been implemented. Note that there may be multiple verification methods, depending on the number of mitigating factors that are used to reduce the risk value for the hazard. For example, for a pressure vessel with a hazard of over-pressurization leading to structural failure, multiple verification methods may be required, including proof-testing, inspection, and verification testing of a relief valve. Here, the highest verification level should be used to define the verification method in the Hazard List.

The following general verification methods in descending order of precedence are identified for each mitigation action that is taken:

Test: functional testing of the installed system is performed to verify that the mitigation method(s) functions correctly to mitigate the hazard

Inspection/measurement: elements intended to mitigate the hazard are visually inspected or measured to verify that they are in place and have been implemented as required

Process control: quality assurance controls are placed on the part or material selection, qualification or proof testing of the articles, and/or fabrication or assembly process controls

Audit: mitigation method is verified by auditing *in situ* that the elements of the mitigation are indeed being used

Review: review or analysis of mitigation plans indicates that mitigation method suitably reduces the hazard level