Large Synoptic Survey Telescope Camera System Plan	Document # **LCA-14-A**	Date Effective 13 Oct 2011	Status RELEASED LCN-001
	Author(s) Martin Nordby Nadine Kurita	Frank O'Neill	
	Subsystem/Office Performance and Safety Assurance		
Document Title **LSST Camera Preliminary Hazard Analysis**			

1. Change History Log

Revision	Effective Date	Description of Changes
A	13 Oct 2011	Initial release. See notice LCN-001.

2. Contents

3. Acronyms and Definitions

3.1. Acronyms

ALARP	as low as reasonably practicable
ATA	Activity Training Assessment
CCD	Charge-Coupled Device
CCS	Camera Control System
CCP	Contamination Control Plan
CD-n	Critical Decision
CFH	Cubic feet per hour
ESD	Electro-Static Discharge
ESF	Engineered Safety Feature
FEB	Front End Board
FEC	Front End Cage
FOV	Field of View
ISEMS	Integrated Safety and Environmental Management System
I&T	Integration and Test
JSA	Job Safety Analysis
LSST	Large Synoptic Survey Telescope
ODM	Oxygen deficiency monitor
O&SHA	Operating and Support Hazard Analysis
PHA	Preliminary Hazard Analysis
POC	Point of Contact
PPA	Particle Physics and Astrophysics directorate at SLAC
PPE	Personnel Protective Equipment
RCC	Raft Control Crate
RSA	Raft Sensor Assembly
SDS	Science Data System
SME	Subject Matter Experts
SOC	Safety Oversight Committee
SSPP	System Safety Program Plan
WIP	Work Integration Plan
WPC	Work Planning and Control

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-31, "LSST Camera System Safety Program Plan"

[3] LCA-15, "LSST Camera Hazard List"

[4] SLAC ES&H Manual

[5] LCA-40, "LSST Camera Integration and Test Plan"

[6] LCA-68, "LSST Camera Environmental Specification"

[7] SLAC-I-720-0A24E-001-R002, "Seismic Design Specification for Buildings, Structures, Equipment, and Systems"

[8] SLAC-I-720-0A00B-001, "SLAC Integrated Safety and Environmental Management System Description;" http://www-group.slac.stanford.edu/esh/general/isems/

5. Purpose and Scope

The purpose of this Preliminary Hazard Analysis (PHA) is to identify hazards associated with the design and operation of the Large Synoptic Survey Telescope (LSST) Camera, assess risk; and establish controls needed to either eliminate the associated risk or reduce it to acceptable levels. Hazards capable of causing injury to personnel, damage to the environment, or damage to critical hardware have been considered in this analysis.

This PHA forms one part of the system safety program defined in [Ref 2], the "LSST Camera System Safety Program Plan," and refers to the baseline design at the time of this report. The hazard reports in this analysis are modified and updated as the design progresses, and an updated version of this analysis is submitted at the Camera Critical Decision-2 (CD-2) Review.

This PHA documents the safety analysis of the LSST Camera design and its operation only. A separate Operating and Support Hazard Analysis (O&SHA) will also be developed for the Camera, which will evaluate hazards introduced into the system by operational and support activities. These include transportation, storage, test, installation, integration onto the LSST telescope, and operation of the camera. The physical and functional interface between the LSST Camera and its attendant fixturing will also be addressed in the O&SHA.

6. Overview

This document is divided into three sections. First, Section 8 describes the process by which hazards are identified, categorized, analyzed, and mitigated. This details the specifics of the process and provides procedural direction for inputting hazards into [Ref 3], the Camera Hazard List. The Hazard List includes all hazards identified by this process along with the mitigation and verification plans. It is used for tracking and managing Camera hazards during the development of the project.

Next, Section 9 describes Hazard Reports. For specific hazards listed in [Ref 3], Hazard Reports are generated to expand on the details in the list to include specifics on the hazard, plans for mitigation, and how the mitigations will be verified. Section 9 describes the hazard reporting process and the minimum required content of a Hazard Report. A hazard report is not closed out until all hazard control measures have been verified. Where system level testing is involved, this may not occur until late in the program.

Section 10 then provides a detailed description of the Camera subsystem major components. The functional description introduces the subsystem and how it functions as part of the larger Camera. A physical description then includes further detail into the basic workings of the components within the subsystem. Finally, the hazard description details the primary hazards associated with the subsystem, separated by the source of energy or originating event. While this lays out the primary hazards, [Ref 3], the Camera Hazard List, describes the details of each hazard explicitly, along with the mitigation and verification plans.

7. LSST Camera Description

The LSST camera is a large aperture optical imager that provide a wide 3.5 degree field of view (FOV) with 0.2 arcsecond/pixel sampling. It is positioned in the middle of the telescope where cross-sectional area is constrained by optical vignetting and where heat dissipation must be controlled to limit thermal gradients in the optical beam. The camera is a fully-enclosed, self-contained assembly, composed of functional sub-assemblies that themselves are modular. The large L1 refractive lens forms the entrance window to the camera. This is followed by the L2 lens that shares a common support structure with L1. The filter is the third optical element, lying just up-beam of the shutter. Five filters are stored on-board the camera in the storage Carousel, while the companion Auto Changer allows for quick filter changes during observing runs. The Shutter lies just behind the filter, providing accurate exposure control and blocking stray light from illuminating the focal plane when closed.

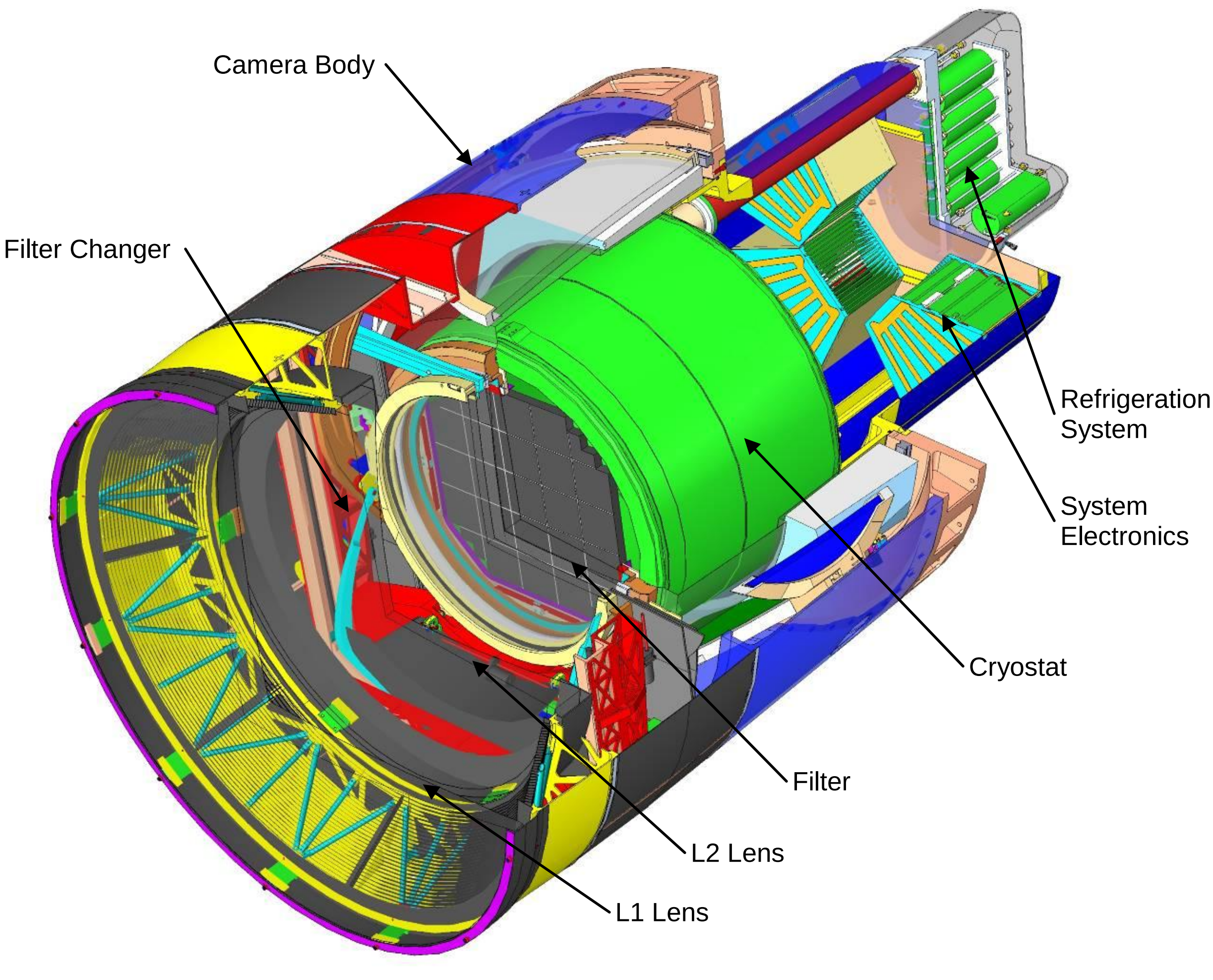


Figure 1: Camera Section View

The fourth and final optical element is the L3 lens, which forms the entrance window to the cryostat and is the final focusing element for the LSST optical system. Just behind this inside the Cryostat lies the 634 mm diameter focal plane. This is comprised of a tiled mosaic of 189 charge-coupled devices

(CCD's), providing approximately 3.2 Gigapixels per image. The detector array on the focal plane operates at -100°C to achieve the desired detector performance. It is contained within an evacuated Cryostat which also houses the front-end analog and digitizing electronics. Within the Cryostat, structural support and thermal and vacuum control systems maintain a suitable operating environment and isolate the detector array on the focal plane from external dynamic and transient loads. The outer camera housing supports the structural loads of the entire 3000 kg camera, cantilevered off of the telescope's rotator, while forming a hermetic envelope around the entire camera to maintain cleanliness, and thermal and environmental control.

Electronics for power conditioning and data handling, as well as cryogenic services are mounted behind the Camera in a Utility Trunk. This also serves as the entrance point for utilities and service lines that are routed up the telescope structure. The entire Camera structure has a diameter of 1650 mm and is over 3.7 m long. Total power dissipated within the Camera is over 2.4 kW.

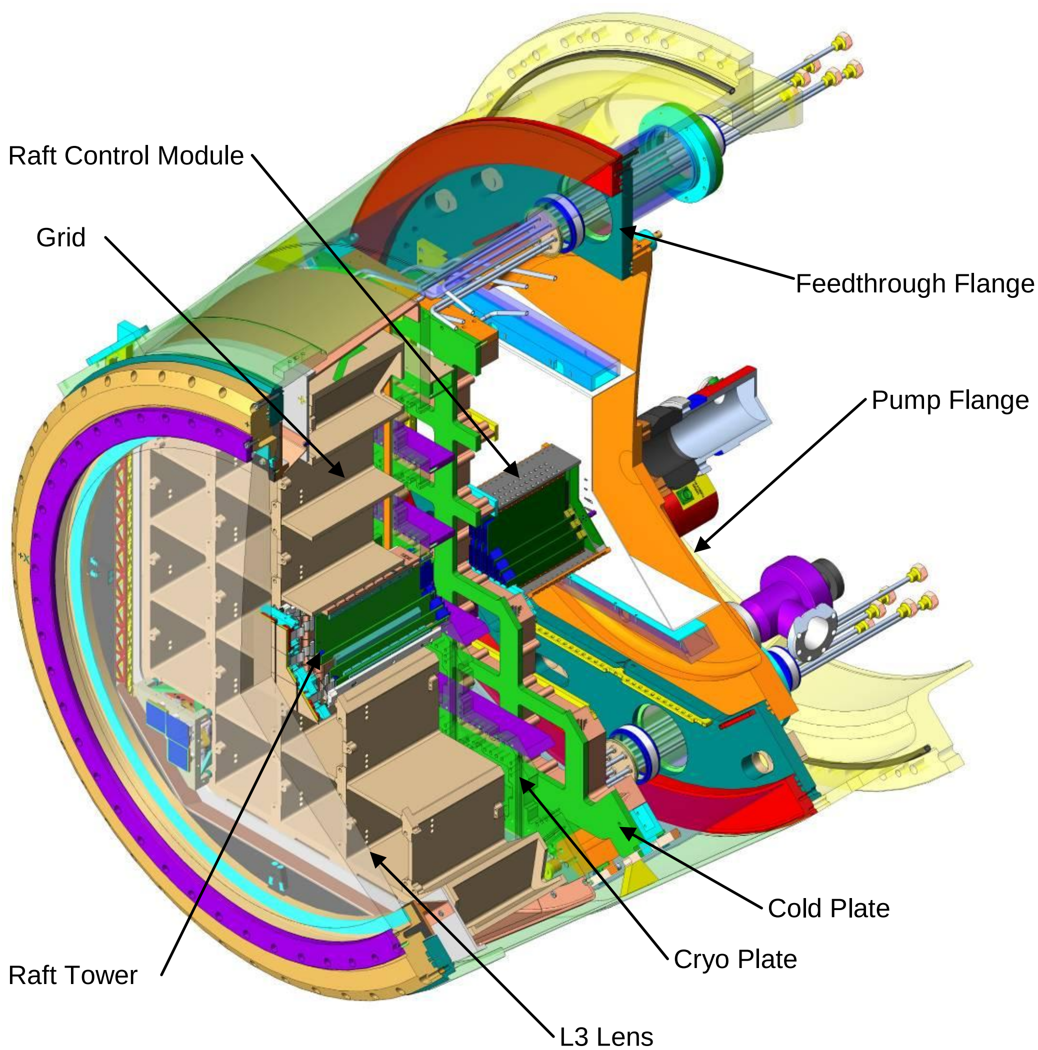


Figure 2: Cryostat Section View

8. Hazard Analysis Process

8.1. Hazard Analysis Process Overview

The hazard analysis process outlined below is a duplicate of the process detailed in [Ref 2], the "LSST Camera System Safety Program Plan" (SSPP). The process serves as the primary means for understanding and managing hazards 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 effectively implemented

This analysis process is qualitative, in that it is based on engineering judgment and weighing of relative risk, and is derived from [Ref 1], ANSI/GEIA-STD-0010-2009, "Standard Best Practices for System Safety Program Development and Execution." It results in three separate sets of information:

System and hazard descriptions: physical and functional descriptions of camera systems, as well as descriptions of the attendant hazards and mitigation plans (included in Section 10 of this document).

Hazard List: a prioritized list, showing all identified hazards along with mitigation and verification plans [Ref 3].

Hazard Reports: reports developed for hazards that may have a significant impact or require more detailed documentation to describe hazards and the mitigation measures (described in Section 9 of this document, with specific Hazard Reports called out in the appropriate hazard entry in the Hazard List).

8.2. 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 is sufficient to allow an adequate characterization of the systems, the associated hazards and their potential impact.

8.3. 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-current, short to ground or other voltage, 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

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. Here, “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 an 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.

8.4. 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

8.5. 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. 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
B	**Probable**	Will occur several times in the life of the Camera
C	**Possible**	Likely to occur sometime in the life of the Camera
D	**Remote**	Unlikely but possible to occur in the life of the Camera
E	**Improbable**	So unlikely, it can be assumed occurrence may not be experienced

8.6. Mishap Risk Assessment Values

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 categorizes, as detailed in Table 4.

Table 3: Mishap Risk Assessment Matrix

	Severity				
Probability		1—Catastrophic	2—Critical	3—Marginal	4—Negligible
	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	Not Acceptable
6-9	Serious	Require decision by LSST Project Office
10-17	Medium	Require decision by Camera Project Manager
18-20	Low	Acceptable without Review

8.7. 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.

8.7.1. 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.

8.7.2. 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.

8.7.3. 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.

8.7.4. Incorporate Safety Device

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.

8.7.5. 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.

8.7.6. 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.

8.8. 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.

8.9. 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

9. Hazard Reports

9.1. Overview

Hazard Reports are used for two primary reasons. First, for hazards with high risk categories or severity, Hazard Reports are used to fully define the hazard, impact, and probability. In particular, hazards which involve multiple sources or initiation points or which could lead to severe consequences are detailed in a Hazard Report. Second, Hazard Reports are used when the mitigation or verification process is suitably complex as to warrant further detail. Here, the Hazard Report provides the process by which mitigation steps are taken, and serves as the focal point for reviewing that all such steps have indeed been taken and verified.

9.2. Hazard Report Details

The Hazard Report amplifies the information already collected in the Hazard List. This includes:

Hazard Number: serial number from the Hazard List

Subsystem: camera subsystem associated with the hazard initiation or stored energy

Hazard Type: type of hazard associated with the stored energy type

Hazard Title: title from the Hazard List

Hazard Description: a detailed description of the hazard

Effects on the System: a description of the result of the hazard coming to pass

Risk Assessment: pre-mitigation risk score, probability, and severity scores from the Hazard List

Hazard Causes: a description of the causes or source of the hazard. Hazards may have multiple possible causes and each should be listed and described separately.

Hazard Controls or Mitigation Steps: details of mitigation plans to control each of the hazard causes as earlier listed. This may include reference to external sources including other reports, analyses, test reports, and the like.

Effects of Mitigation: describe the results of the mitigation in reducing the probability or severity of the hazard coming to pass.

Verification Plans: detail the plans and procedures for verifying that all mitigating actions and controls have been taken. Separate these plans by hazard cause. Ultimately, this should include references to final verification test reports, procedures, and other documentation to demonstrate that all mitigations have been taken and the hazard is mitigated as planned.

10. LSST Camera Hazard Description

10.1. Overview

The following sub-sections contain detailed descriptions of each camera subsystem element. The sections are separated into three sub-sections. First, there is a functional description of the use and function of the subsystem element. Second is a physical description of the hardware, including a description of basic components and their function, special materials, and key interfaces. Third is a description of the potential hazards organized by hazard type, including risks to hardware, personnel, and the environment from these sources. This also includes risks that the hardware poses to other hardware, personnel, or the environment. This is for all phases of manufacturing, integration and test, operations, and servicing.

Hazards are organized by hazard type, defined as energy source or initiating event or condition that produces the hazard. The following types are used:

Thermal and Cryogenic: overheating, extreme cold, temp rates of change

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

Mechanical: collision, dropping, loss of function, mechanical failure, personnel injury

Structural: collapse, deformation, sensitivities to vibration/shock/noise (including due to seismic activity)

Electrical: over-current, short to ground or other voltage

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 or release of—or exposure to—materials which can damage equipment, cause environmental harm, pose health or safety risks to personnel

Contamination: damage to equipment due to unplanned exposure to contaminants

Camera subsystem elements are:

Optics: L1, L2, and L3 lenses and filters

Filter Exchange system: storage Carousel and Changer systems

Shutter: including light baffling

Cryostat assembly: cryostat vessel, Grid support structure, thermal control and vacuum systems

Refrigeration system: on-camera and ground facilities for low-temperature refrigeration system

Science Raft Towers: CCD detectors and their support Rafts; front-end analog electronics module; back-end Raft Control Module

Corner Raft Towers: wavefront and guide sensors and their support rafts; separate front-end and back-end electronics

System electronics: power conditioning and distribution; timing, control and data handling electronics

Camera body: housing, support flange, and support structures; purge gas and temperature-control system

10.2. Optics

10.2.1. Functional Description

The camera optics design includes four optical elements. First, the large L1 and L2 refractive lenses are mounted at the entrance to the camera, and minimize chromatic effects of L3 and the filters. These are followed by interchangeable broad-band filters. Five filters are stored on-board the camera, allowing for quick filter changes during observing runs to provide spectral coverage from the ultraviolet to near-infrared. Finally the L3 lens serves as a window and vacuum barrier for the cryostat containing the cooled detector array.

10.2.2. Physical Description

10.2.2.1. L1/L2 Assembly

The large L1 and L2 lenses are housed in a separate sub-assembly at the front end of the camera. The L1 lens has a clear aperture radius of 775 mm and forms the window into the Camera volume, with a diameter nearly that of the Camera itself. With a clear aperture radius of 551 mm, L2 is significantly smaller in diameter, but still large and heavy. The two lenses are supported off a toroidal ring with a triangular cross-section. Each lens is mounted to the ring by way of flexures which isolate the lenses from forces and moments due to distortions of the ring and changes in temperature, while providing azimuthal and axial positioning. The entire sub-assembly is kinematically supported off the front end of the camera housing by a hexapod of adjustable struts. The struts provide a stiff support to minimize gravity-induced deflection, while also reducing motions due to changes in temperature. They include flexures at either end to reduce bending forces, and differential-screw adjusters to provide fine-adjustment capability without sacrificing strength or stiffness.

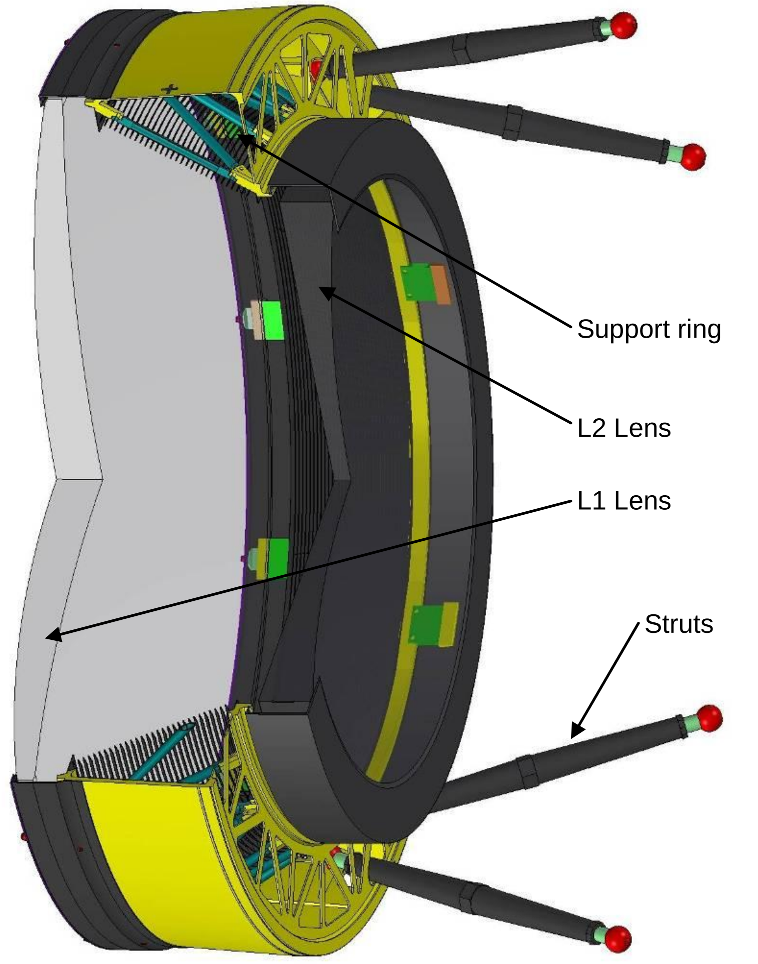


Figure 3: L1-L2 Assembly

10.2.2.2. Filter Assemblies

The filter assemblies include the 375 mm radius glass filter supported and captured by a structural support frame. The optic is held and aligned by this frame, which in turn is supported by the filter exchange system. Given the space constraints, flexures are not used, but the glass is sandwiched between O-rings to allow for relative radial thermal expansion of the frame with respect to the filter, while still providing stable support and alignment. Multiple layers of coating are sputtered onto the glass substrate to produce the unique wavelength passband for each of the filters.

The filter assembly is supported by the filter exchange system. While on-line, the two trucks of the Auto Changer hold the filter with a simple kinematic mount system on either side of the filter. Likewise when the filters are off-line in storage on the Carousel, they are mounted to the Carousel structure with a kinematic mount and retainer system.

10.2.2.3. L3 Lens Assembly

L3 is the smallest lens, with a clear aperture of 690 mm. The L3 lens also forms the vacuum barrier for the cryostat containing the detector array, which is spaced 28.5 mm off its inner surface. As with the filters, the L3 lens is supported in a frame which in this case also forms the front flange of the cryostat. The vacuum side of the lens rests on a viton gasket around its perimeter which both forms a vacuum seal and carries the vacuum load of the lens. The gasket is thick enough that it shears to accommodate the differential expansion between the flange and lens. On the air side of the lens, a clamp ring with O-ring captures the perimeter of the lens.

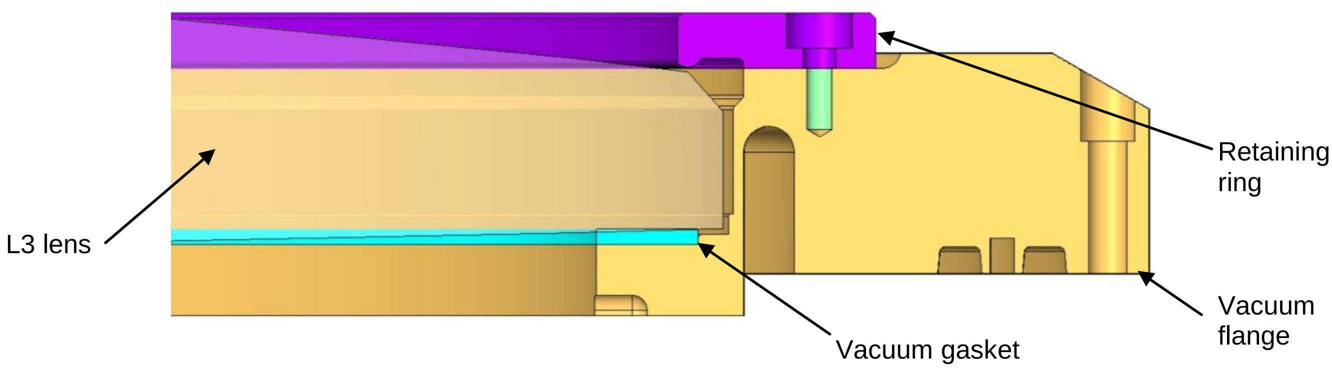


Figure 4: L3 Lens Flange Assembly

10.2.3. Hazard Description

10.2.3.1. Thermal and Cryogenic

The L3 lens has an unobstructed view of the -100 ^{o}C detector plane, which cools the lens by radiation heat transfer. This could either embrittle the glass or cause thermal contraction beyond the range of accommodation of the perimeter gasket. In either case, this may generate stresses in the glass above allowable limits which could ultimately result in failure. This risk has been assessed by analyzing the black-body radiative cooling load, which is the maximum radiative heat transfer possible. However, even these worst-case condition do not pose a hazard to the lens.

The L1 lens is exposed to the dome environment inside the telescope, so it may experience temperature extremes of the mountain-top environment. Such extremes would produce relatively large differential radial expansion/contraction between the lens and its support ring, which stresses the flexures that bridge between them. Overstressing these highly-loaded flexures could ultimately result in failure. However, this risk has been eliminated by designing the flexures to survive a temperature range much larger than they should ever see. Thus, the flexures pose no hazard to the camera, even when exposed to the worst-case temperature extremes expected at the summit.

10.2.3.2. Pressure/Vacuum

During operation, both the L1 and L3 lenses are exposed to pressure—and vacuum—differentials which stress the glass. For each of these loading scenarios, there is the possibility of overload due to overpressure, which could cause the lens to fail. This hazard is being mitigated by designing for the maximum pressure differential, and by providing relief valves to ensure that the volumes never exceed their rated pressure

Another pressure-related hazard is failure of the vacuum gasket that supports the L3 lens, which could result in an uncontrolled venting of the cryostat, possibly introducing contaminants or water vapor into the cryostat and damaging the detectors. However, the vacuum gasket—and the back-up O-ring—are designed and will be tested to tolerate the vacuum load combined with the shearing produced by contraction of the flange relative to the lens.

10.2.3.3. Mechanical

Filter collision may occur due to a failure in the Filter Exchange system. This hazard is reviewed in the Filter Exchange section.

The L1 lens is open to the dome and is at risk of damage by personnel or equipment during access to the Camera. This hazard is mitigated by using a lens cap to cover up the lens during extended accesses, and by accessing the camera from the side, so there should be little opportunity to contact the lens.

The L2 lens is fully within the camera housing. However, to remove the Shutter or Auto Changer from the camera, the region between L2 and L3 is accessed by personnel and handling hardware. During such an access, there is a risk that personnel, tools, or handling fixtures contact the L2 second surface, damaging either the coating or even scratching the lens. To protect the lenses, rails are used for removing the Shutter and Auto Changer and a cover can be installed to completely cover L2.

10.2.3.4. Structural

The L1-L2 assembly could be exposed to distortions imparted on the assembly by distortions in the rest of the camera. However, the kinematic hexapod support ensures that no loads can be transmitted into the L1-L2 assembly. Similarly, the filter frame could be overloaded if the Auto Changer jammed or encountered some serious problem. However, the kinematic mount of the filter frame on the changer trucks will prevent any overload.

A flaw or micro-crack in the glass could cause a failure in L1 or L3, the two lenses that are under stress due to pressure loads. This risk is mitigated in two ways. Fracture analysis is performed to establish the maximum allowable crack size. The lens is then inspected to verify that there are no cracks of that size. If needed, this inspection can be repeated if a problem is suspected.

10.3. Filter Exchange System

10.3.1. Functional Description

The camera houses five on-board filters for fast filter changing during nightly viewing, and includes the capability for swapping in a sixth filter during a daytime maintenance access. As shown in Figure 5, the filter exchange system includes three sub-assemblies to provide this functionality. The Carousel holds the filters that are not in use, and moves filters into position for placing them on-line when needed. The filters sit in cradles on a ring bearing that surrounds the cryostat, with the filters oriented 90 degrees to their on-line position. The selected filter is moved into the light beam by the Auto Changer. This mechanism shuttles the filter from its slot in the Carousel, forward and around the edge of the cryostat and L3 lens, to the on-line position between the L2 and L3 lenses.

Finally, a Manual Changer is used for swapping out a filter during daytime access. The Manual Changer engages with the internal auto changer rails to ensure a smooth and safe hand-off of the filter. All three of these assemblies ensure that the large-diameter filters are handled safely, and can be accessed and brought on-line quickly to maximize viewing time.

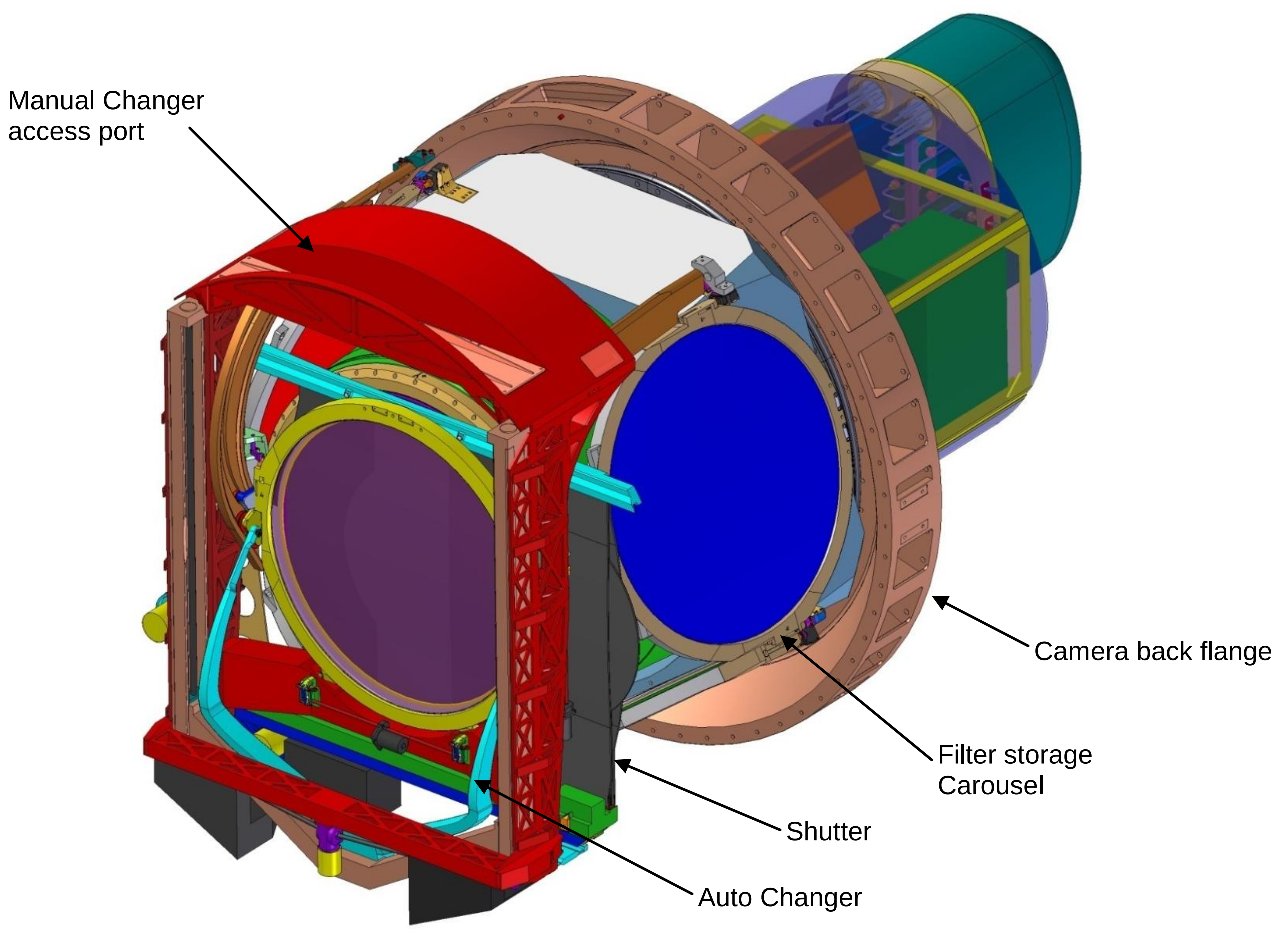


Figure 5: Camera Partial Assembly Showing Filter Exchange System

10.3.2. Physical Description

10.3.2.1. Carousel

The Filter Carousel supports filters inside the camera body when they are not in use in the field of view (FOV). Each filter has a clear aperture diameter of 690 mm, and the heaviest has a mass of 35.5 kg. The Carousel can support from zero to five filters, accommodating any filter in any azimuthal location, or "socket." The filters are mounted around the perimeter of a large ring bearing. The fixed inner ring of the bearing mounts directly to the camera back flange, while the rotating outer ring supports the posts and clamps that hold the filter frames. The outer ring also supports the large ring gear that is used for rotating the Carousel to place the selected filter in the stand-by position in preparation for moving it on-line.

Motor(s) drive the Carousel by way of pinion gears and possible further gear reduction. The motors fit in cut-outs in the back flange of the camera. More than one motor may be needed, arrayed around the perimeter of the Carousel, to provide the required torque and power in the relatively small volume available. The reduction gearing for the motor, if any, are non back-drive-able, to prevent uncontrolled rotation of the Carousel if power is lost, and to hold the Carousel in position. If gearing is not adequate to do this, the Carousel will also need a brake. This could either be mounted on the motor drive shaft, or engage the rotating ring directly, but must stop all Carousel motion in the event of loss of power. The Carousel can be rotated in either direction, to shorten the travel distance and reduce the time to exchange a filter. Encoders or other sensors monitor the position of the Carousel during rotation, to provide location information after a loss of power or control.

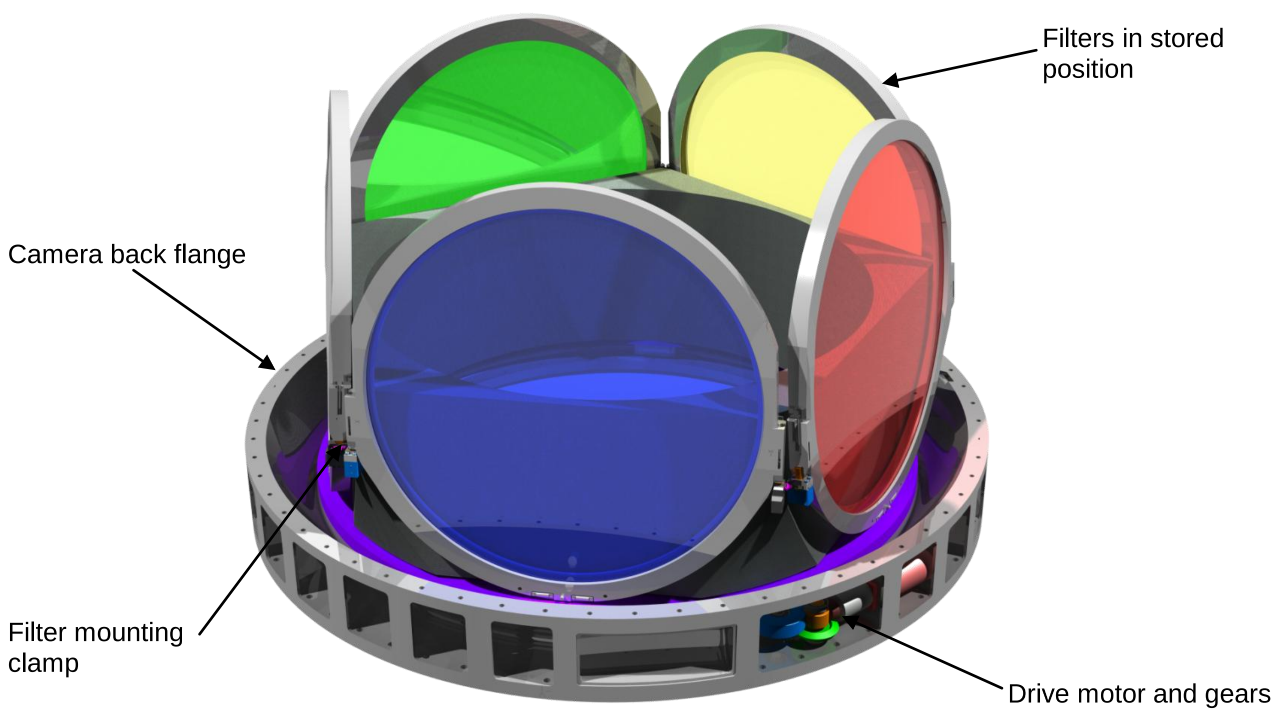


Figure 6: Filter Storage Carousel Mounted to Camera Back Flange

The five filter clamps are mounted on posts that are supported off of the rotating ring of the Carousel. The clamp mechanism is spring-loaded and normally clamped, ensuring that the filters are held in place even during a power failure or loss of control signal. The clamp block and mechanism must securely hold the filter during all operational and seismic accelerations and in all standard camera attitudes, while maintaining filter alignment to ensure that it can be successfully picked up by the Auto Changer trucks.

The Carousel includes filter clamp release mechanisms that release the spring-loaded clamp after the filter is grabbed by the Auto Changer trucks. This release mechanism is normally disengaged, so power is required to engage it and release a filter clamp. One release mechanism will be mounted to the camera housing opposite each filter clamp at the stand-by location, and used for releasing any of the filters.

10.3.2.2. Auto Changer

The Auto Changer moves a selected filter from its stand-by position in the Carousel to the on-line position in the field of view of the camera optics. The filter is moved along two fixed rails by trucks that roll on the rails and support the filter on either side of its equator. Each rail is comprised of two sets guide tracks, with one set supporting the weight of the filter and the second set providing control of the filter angle. As the filter is pulled away from its stand-by position on the Carousel, the spacing between the two sets of tracks on the rail changes, thereby tipping the rail and rotating it as it moves around the corner of the cryostat and into its on-line location. By varying the spacing of the tracks on the rails, the filter tip angle is tied to the linear position of the filter along the rail. This eliminates the need for a tip-angle actuator and the attendant additional complexity. As a result, the Auto Changer includes only one actuated degree of freedom, which is provided by a linear slide and ball screw, with a linkage to tie the linear actuator to the trucks that ride along the curved rail profiles.

The Auto Changer is driven by a single motor with gear reducers and drive shafts running to two sets of linear slides and ball screws which straddle either side of the camera FOV. The single motor could be replaced with two smaller motors—one for each slide—which are electronically controlled to move the slides in unison. Two driven slides are used to ensure that the filter cannot jamb or get wedged in place, as can happen when driving from one side only (akin to closing a dresser drawer while pushing from one edge of the drawer). The drive train cannot be back-driven, to ensure it is safe from loss of power. This will likely be done by using a worm-gear speed reducer, but may be performed with a brake either on the motor shaft or on each ball screw shaft.

The carriages on the two linear slides are joined by a yoke that bridges across the FOV and provides a common central pivot point for the linkage that connects to the trucks that ride on the curved rails. While the slides are long enough to provide the full range of travel needed for a filter, their positions are constrained by the outer diameter of the camera housing. The housing effectively centers the slides on the center of the camera, which is not ideal to cover the entire range of motion of a filter. Thus, the yoke serves to offset the pivot point of the linkage to one side of the camera, which allows the slides to move the filter all the way into the FOV on the camera centerline. As the filter is moved off-line to its stand-by position on the Carousel, the linkage pivots to push the filter around the corner of the cryostat and back along the rail to the Carousel.

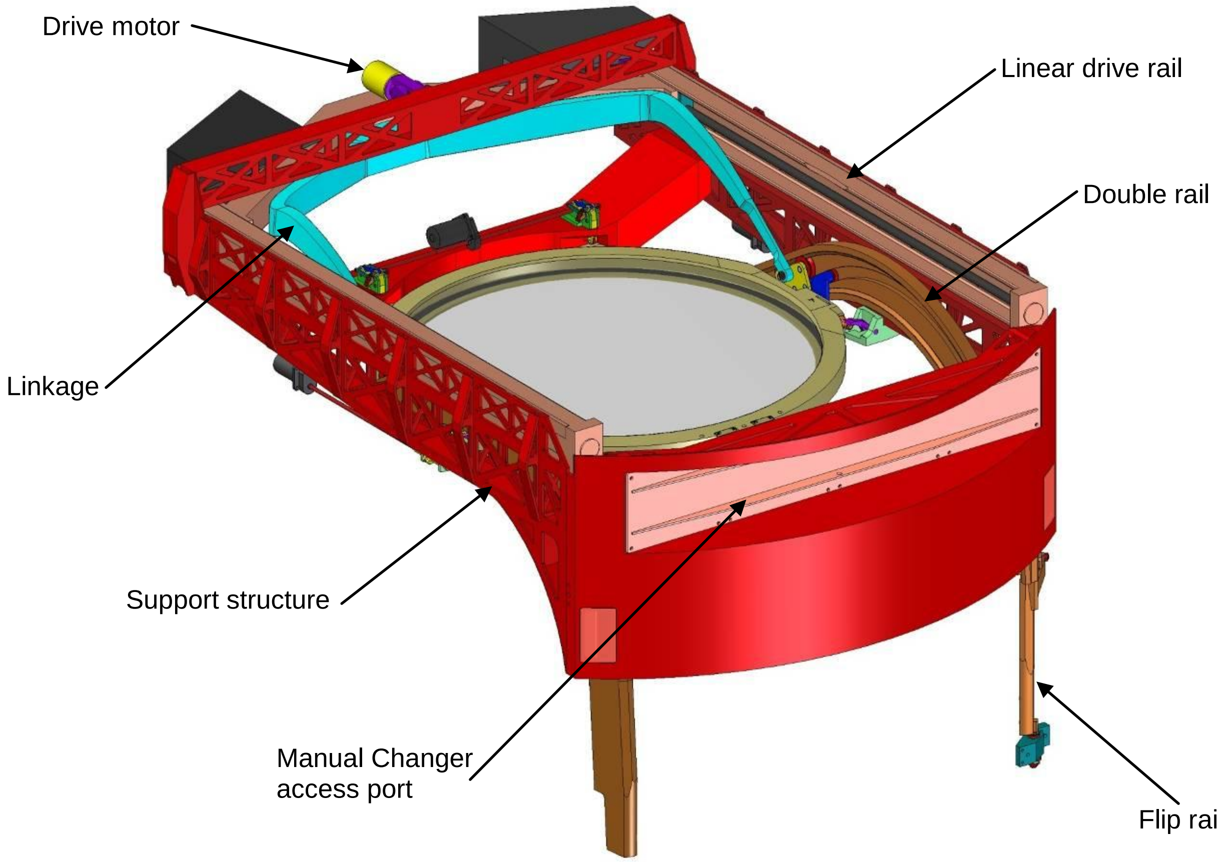


Figure 7: Filter Auto Changer with Filter in On-Line Position

The C-shaped linkage mounts permanently to the two trucks with a rod end to allow the trucks to pivot and to provide compliance of the joint to accommodate small misalignments and reduce the likelihood of wedging the filter. The trucks include four wheels, three of which support the weight of the filter and guide it along the track. The fourth sits on a pivoting arm extending off the truck and rides in the second track of the rail. This provides the angular rotation for the filter. The trucks also include a key and spring-actuated latch that runs into a slot on either side of the filter. The spring-actuated latch prevents the filter from sliding off the key, and is actuated with an actuator to disengage the filter. This ensures that the filter support mechanism is safe against loss of power, and the control system ensures that the latch release can only be activated when the Carousel clamp is engaged.

The trucks roll along the rails to move a filter to the stand-by position on the Carousel. They also can operate without a filter, to back away from the Carousel in preparation for rotating the Carousel. After the empty trucks are backed away, the backward-most sections of the rails are flipped flat against the outer housing of the camera, to clear the path taken by the filters as they rotate in the Carousel. This simple flipping motion is likely handled by a double-acting solenoid which overcomes a pivot mechanism which is stable with the rails either flipped flat or aligned with the remaining rails. This ensures that the rails hold their position in a power or control failure.

The Auto Changer is supported off of the camera body by two structural beams that bridge across the enclosed volume. Each beam supports a rail and linear slide, with the entire assembly pre-aligned and integrated as a unit. Light baffles are also mounted to the support beams, to shield all components from reflecting any stray and scattered light, and to define a clean circular clear aperture for the beam as it passes through the filter.

10.3.3. Hazard Description

10.3.3.1. Thermal

The motors and actuators that drive the Filter Exchange mechanisms are used only intermittently, so the average heat load is low and heat is removed by air flow. While the mechanisms are in use, power consumption is higher, but the thermal mass of the motor and its mounting brackets absorbs the heat for the short amount of time. If the Carousel or Changer drive system were to stall due to some mechanical failure, the motor would heat up. However, this would only be temporary since the position and force/torque feedback instrumentation would stop the motor. Thus, overheating of the motor or other actuators is not considered a hazard.

10.3.3.2. Mechanical

The Filter Exchange system uses a variety of mechanisms to perform its function, and loss of function of either a mechanism or monitoring instrumentation can result in hazards to the equipment or personnel. These hazards are discussed here, grouped into the following classes: collision, dropping, mechanical failure, and personnel injury.

First, the filter exchange system uses mechanisms and instrumentations that must function correctly and be controlled to follow prescribed actions only when the system is in a state that is known to be safe for the action to be executed. If an action is inadvertently executed while the system is in a state that is not safe for that action, physical collisions of parts could occur. Examples of this include: moving the filter to its parked position while the Carousel is not rotated into its correct orientation; rotating the Carousel while the flip rails are not lying flat; driving the Changer trucks off the ends of the rails if the flip rails are lying flat; driving the filter into its on-line position with the clamps engaged. Any of these actions would likely result in damage to the mechanisms and possibly to a filter as well. This hazard is being controlled by using instrumentation to monitor the state and position of every moving mechanism. Commands can only be executed if all sensors provides positive indications that mechanisms are in their correct location. This will protect against "operator error" of commanding an action that should not be executed, and ensure that an action cannot start until the prior action has been successfully completed. All instrumentation must provide a positive signal to enable an action, so loss of signal from a switch or monitoring device will disable the actuators—eliminating the possibility of "driving blind."

The second mechanical hazard is inadvertent dropping of a filter at the hand-off between the Carousel and Auto Changer. While this is perceived to be the biggest worry for the system, qualitatively it falls into the same class of hazard as a collision: loss of knowledge of the state of the hardware. As with collision hazards, the dropping hazard is being mitigated by using instrumentation to monitor the condition of each clamp that is used for holding the filter. For the clamps, in particular, limit switches monitor both the open and closed state of each clamp, to ensure that a filter is neither dropped nor moved with both sets of clamps still engaged.

Mechanical failure, the third class of hazard, is the broadest class and most difficult to mitigate. Given the function of the mechanisms, some parts are single-point failure parts where loss of function or outright failure could damage the system. These include the axles for the flip rails, filter latches, and wheels on the trucks, and keys and retaining pins for the motor drive shafts and linkage. For all of these parts, we will use parts designed with large factors of safety, and proof test all hardware prior to use.

Degradation of other components could result in a “softer” failure or prolonged decrease in performance that could ultimately result in a system failure. These include wear or damage to bearings in the trucks and in the carriages for the rotation mechanism in the Carousel and linear actuators in the Changer. Gradual degradation of performance could indicate wear that may result in failure if ignored. We have three methods to mitigate such a hazard. First, prototype testing will provide empirical data for establishing maintenance intervals for the moving components. This preventative maintenance should eliminate the possibility of parts wearing excessively. Second, we will monitor trends in the performance of the systems by collecting data on motor currents to look for slow changes that could signal an impending problem. Finally, if a failure of some kind does somehow occur, over-current trips on the motors will stop the actuators before any secondary over-loading can occur.

The final class of mechanical hazard in the filter exchange system is injury to personnel working around the system. The Auto Changer, in particular, has a number of pinch points and apertures that open and close, many of which are relatively exposed to personnel who are either integrating and testing hardware initially, or performing routine maintenance or troubleshooting. Given that the heaviest filter has a mass of 35 kg, the force required to move the filters is large, which could result in injury.

A lock-out/tag-out system is used to disable all mechanisms in the filter exchange system when personnel are working around it. This administrative control provides for a safe working environment for personnel working around the system. For people actually working on the filter exchange system, we are investigating a few options. First, we will have a “panic button” available to cut power to all mechanisms. This could either be in the form of a dead-man’s switch or a push-button. Also, we are currently investigating engineering solutions to add safety features such as wipers, finger blocks, and other guards to reduce pinch hazards, in particular. Finally, we will look into adding feeler switches or continuity switches that detect when anything brushes up against a moving mechanism in a potential pinch or crush area. This would stop actuators if anything encroaches on the area.

10.3.3.3. Structural

Structural loads in the filter exchange system are generally small, relative to the dimensions of the members. The sole exception is the pivoting C-shaped linkage that transfers the linear motion of the actuators to the curved motion of the trucks that follow the path of the rails. The linkage is pinned at both ends, so there are no bending moments imparted on it. However, the relatively thin members will experience high axial loads along the line of action between the pinned joints that result in bending and twisting of the members. Furthermore, the loads can be both tension forces or compression, so buckling is a consideration. Structural failure or buckling of the linkage would likely stop the trucks in their tracks, but may also damage either the filter or even the neighboring Shutter, depending on the direction the linkage failed.

Structural failure of the linkage is being mitigated by using closed sections to improve its stiffness against twisting and buckling. Also, the linkage will be proof tested to qualify the safe working load of the design, especially relative to its calculated buckling force.

10.4. Shutter

10.4.1. Functional Description

The shutter for the LSST camera lies tightly packaged between the L3 lens/cryostat window and the filter. It controls the length of time that the sensors on the focal plane are exposed to an image while blocking out all stray light when closed during read-out of the CCD sensors. The shutter is a double-acting guillotine-like device, where flat plates move across the focal plane to start or end an exposure. This double-acting shutter essentially includes two shutters. The first moves off to one side to clear the FOV to start the exposure, then the second shutter occludes the FOV by coming on from the opposite side, and traveling in the same direction as the first. For the next exposure, the process is reversed. This provides a more uniform exposure time for all pixels, since the first pixel exposed by the trailing edge of the first shutter is also the first blocked by the leading edge of the second.

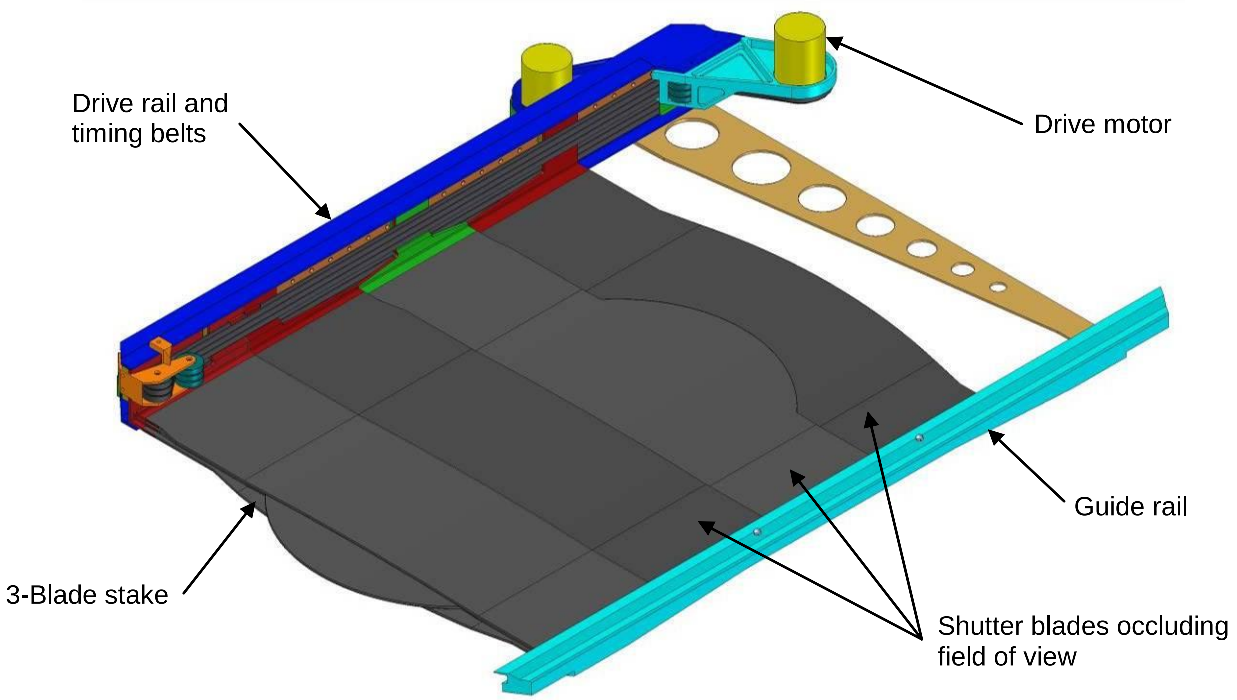


Figure 8: Shutter Assembly

10.4.2. Physical Description

Double-acting guillotine shutters have been used on a number of cameras, but tight lateral space constraints have forced us to segment the one-piece shutter into three flat blades which are stacked up when the shutter is open, then slid over the field of view in a coordinated telescoping motion to close. The three blades are three-dimensional shapes, manufactured from carbon-fiber face sheets and a high-density foam core. The blades are supported at both ends, but only driven from one end, where they each are supported by separate carriages on a single rail. The carriages are attached to a single drive motor by way of separate timing belts that wrap around timing pulleys of differing diameters, moving the three blades in unison but at different speeds. Thus, a single motor drives all three blades to extend and retract over the entire FOV.

Likewise the opposing stack of three blades shares the same rail—six carriages on a single rail—and includes its own drive motor and pulley set. A single rail is used for all six blades, since only one set of blades covers the field of view at a time. This uses the minimum number of components to drive the blades, while ensuring that the timing requirements are met by implementing proven timing-belt technology that has been used in the automation industry for many years.

10.4.3. Hazard Description

10.4.3.1. Mechanical

The shutter is comprised of moving parts, so mechanism failure constitutes the primary hazard associated with the component. Given the proximity of the L3 lens to the moving shutter blades, one hazard is that a blade could contact the lens and scrape it, thereby ruining its optical quality. To reduce the likelihood of this happening, the shutter blades are guided from both of their ends by carefully aligned rails and the blade design will be tested to ensure that it does not flutter or vibrate. We are using a stiff carbon fiber lay-up with a very light foam core, to minimize weight and maximize stiffness and damping, all of which serve to reduce dynamic vibrations.

Another hazard is of blades colliding with each other. Since we have two sets of blades running on the same track, there is a risk that both blade sets are actuated simultaneously and collide in the center of the aperture. If this were to occur, the shutter blades would be damaged, and the L3 lens would likely be scratched, as well. This is prevented by fail-safe monitoring of shutter blade position. Thus, one blade set cannot be actuated unless there is a positive signal that the other set is out of the way. Since only one blade set moves at a time, we can ensure that the path is clear prior to actuating either set of blades. This also protects against a failure of a timing belt in one of the blades. Such a failure could strand a blade in the middle of the aperture or even allow it to fall back to the lower end of its travel. If this were to happen, the limit switch at the blade's end of travel would not close, which would dis-allow any further motion of either set of blades.

The final mechanical hazard is a pinch hazard for personnel. Since the blades occlude an aperture, there is a possibility that a finger could get pinched by the closing blade. We expect to have shields to deflect objects out of the path of oncoming shutter blades, and will also use administrative controls including lock-out/tag-out procedures and protective covers to reduce the possibility of a pinch from occurring.

10.4.3.2. Structural

The shutter is supported at its four corners off of the camera housing, and is intentionally designed to be somewhat flexible to reduce over-constraint forces. Also, it is very light, so forces and stresses on components will be very low. Thus, we do not anticipate any credible structural failure scenario for the shutter.

10.5. Cryostat Assembly

10.5.1. Functional Description

The cryostat lies at the center of the camera. Its vacuum housing supports the detector plane of CCD detectors that operate at -100 ^{o}C, as well as the analog and digitizing electronics. The cryostat assembly serves three functions: providing structural support and isolation for the detector plane, maintaining thermal control of the detectors while removing the dissipated and radiative heat load, and ensuring that the detectors are in a clean operating environment.

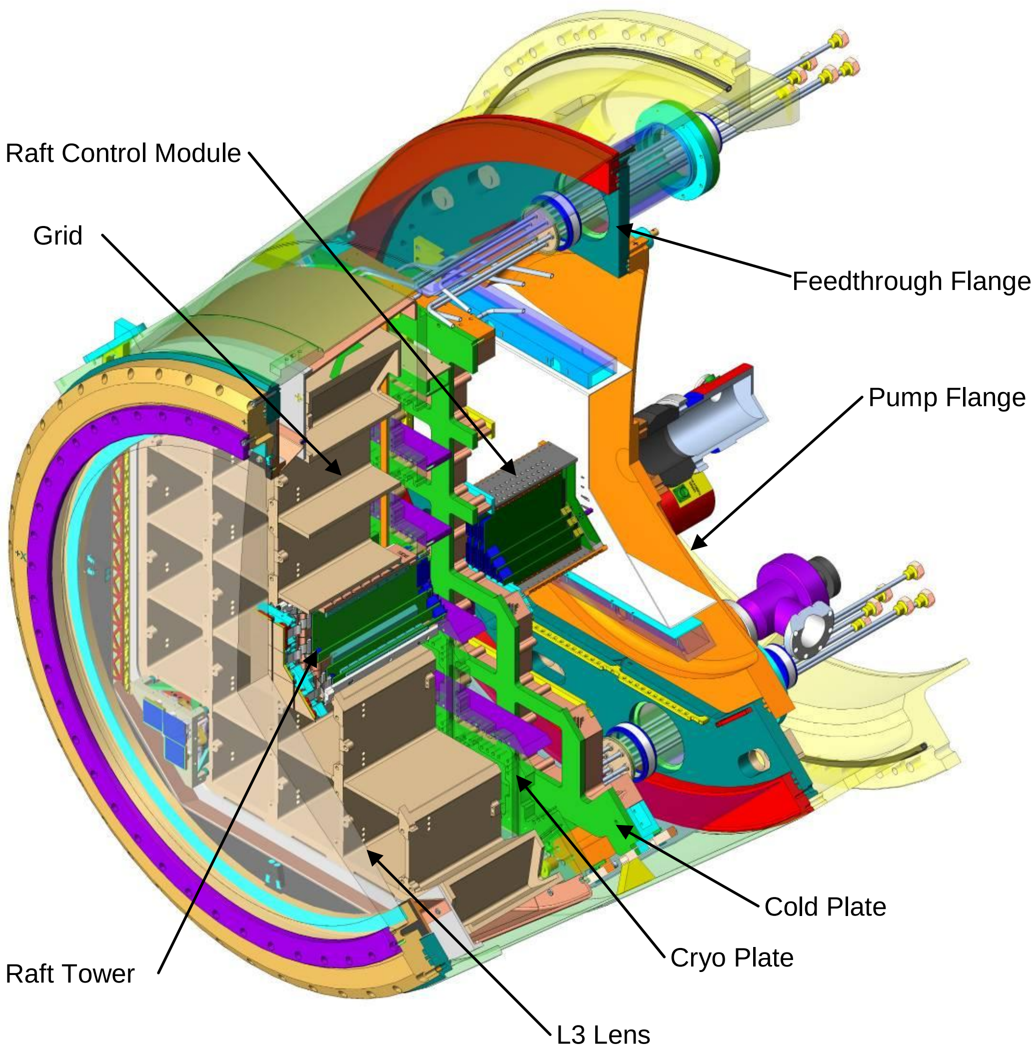


Figure 9: Assembled Cryostat with Raft Tower Inserted

The cryostat is comprised of a conical-shaped vacuum housing, capped on the front end by the L3 lens assembly, and on the back end by feedthrough and utility bulkheads. Flexures mounted to the housing support the Grid assembly which stably supports and thermally isolates the CCD detectors on their rafts. Behind the detector plane, the actively cooled Cryo Plate removes process heat loads from—and provides structural support for—the front end electronic modules, while providing a stable thermal environment for the Grid and detectors. Further back in the Cryostat, the cold plate similarly supports and cools the digitizing and control electronics. At the back end of the Cryostat, image video and instrumentation signals pass through vacuum feedthroughs in the back flange, along with cryogenic lines. Vacuum pumps and instrumentation are also located here, to help maintain the clean, cold environment.

10.5.2. Physical Description

10.5.2.1. Cryostat Housing

The Cryostat housing provides vacuum containment and structural support for all of its contents. The conical housing includes support bosses for the Cryo and Cold Plates. A welded flange on its front end provides the mounting and vacuum sealing surface for the L3 lens assembly as well as the structural support for the Grid support flexures and molecular sieve getter pumps. The housing is tapered to allow for more efficient flow of stresses, thereby reducing peak stresses and minimizing deflections due to gravity. At the back end, the housing bolts to a support cylinder that is cantilevered off of the camera back flange.

10.5.2.2. Grid Assembly

The Grid assembly provides stable support for the CCD detector rafts. The silicon-carbide structure has a high stiffness-to-weight ratio, high thermal conductivity, and low coefficient of expansion, making it the ideal material to meet the structural stiffness and distortion requirements. Ball nests mounted to the Grid form the kinematic interface to each of the detector rafts, while cold straps in each Grid bay ground the Grid thermally to the Cryo Plate. The Grid is supported off of the Cryostat front flange by three titanium flexures that provide kinematic support and thermal and electrical isolation.

10.5.2.3. Cryo Plate and Shroud

The Cryo Plate structurally supports and cools the front end electronics, while also providing a stable thermal environment for the Grid. The large copper plate includes stainless steel stiffening ribs to carry the weight of the electronics, and cooling channels for flowing refrigerant to remove the heat dissipated by the electronics. A cryo shroud mounts to the perimeter of the plate and extends forward around the outer and front faces of the Grid, isolating it from radiative heating from the warm walls of the Cryostat housing. The Cryo Plate and shroud assembly mount to the Cryostat housing by four titanium flexures, while refrigerant supply and return lines enter and exit the Cryo Plate from vacuum-insulated feedthroughs at the rear of the Cryostat.

10.5.2.4. Cold Plate

The Cold Plate structurally supports and cools the digitizing, communication, and control electronics. This is also a large copper plate, cooled with a cryogenic refrigerant. It is also supported off the Cryostat wall by four titanium flexures shared with the Cryo Plate.

10.5.2.5. Cryostat Back End

The back end of the Cryostat includes an annular feedthrough flange, pump plate, and pumping plenum. The plenum connects the turbomolecular pumps to high-conductance pumping chimneys tied into the region around the detector plane, and is removable to provide clear access to the backs of the raft control crates. Additional pumping is provided by cold-activated charcoal getter pump cartridges which reside within both chimneys and zeolite getter cartridges mounted at the front of the cryostat.

The annular feedthrough flange mounts to the back end of the Cryostat housing, forming part of the vacuum wall of the Cryostat. It includes bolt-on electrical and optical feedthroughs with O-ring seals for all instrumentation and control of components in the Cryostat. Both the flange and the individual feedthroughs have double O-rings with intermediate pump-out grooves.

The pump plate bolts and seals to the feedthrough plate, closing out the Cryostat vacuum wall. This plate supports turbomolecular vacuum pumps, a residual gas analyzer, and other vacuum instrumentation for the cryostat, as well as valves for venting and pumpdown.

10.5.3. Hazard Description

10.5.3.1. Thermal and Cryogenic

The Cryo Plate, Grid, Cold Plate, and components mounted to them operate at cold and cryogenic temperatures. A significant hazard to these components is loss of temperature control, leading to temperatures exceeding normal operating ranges. On the cold end, components could be over-cooled and possibly fail, but during room-temperature testing components could be overheated if coolant is lost. At both extremes, this hazard is handled by temperature sensors on the Cryo and Cold Plates to ensure they do not exceed their operating ranges, as well as sensors on the electronics to track temperatures while the units are operating.

10.5.3.2. Pressure/Vacuum

The Cryostat is evacuated during normal operation. However, failure of an O-ring seal, a leak through a feedthrough pin, or a leak across a welded seam in the housing could result in an uncontrolled venting of the volume. Such a venting could introduce contaminants and water vapor into the clean Cryostat, which would freeze onto the cold CCD’s. Also, a rapid venting may produce large pressure differentials across components in the cryostat, leading to unexpected loads on components.

The risk of uncontrolled venting is reduced by using double O-ring seals with an intermediate vacuum groove at all bolted joints. Thus, the failure of one of the seals can be detected immediately and repair plans put in place, while the second seal is still functioning. Furthermore, both the Cryostat vessel and every feedthrough will be pressure-tested and leak-checked prior to use. Finally, the Cryostat is surrounded by the clean camera volume, so any possible accidental vent would ingest very clean and dry gas into the cryostat.

10.5.3.3. Structural

Components in the Cryostat are subject to four possible sources of structural failure. First, the large temperature differences in the Cryostat can lead to high stresses from differential contraction. We are reducing this risk by using flexures to support the Cryo and Cold Plates, and the Grid. Components will also be analyzed and tested to ensure that any cool-down stresses are within allowable limits.

Structural failure hazards can originate with brittle materials failing prematurely. Some materials may embrittle at cold temperatures, while the Grid is manufactured from a ceramic, which tends to be less fracture-tough than most metals. In both cases, brittle failure hazards are mitigated with a conservative test program to ensure that even under worst-case conditions the material is not stressed to failure.

Non-linear failures can also occur with buckling of the cryostat vacuum housing under combined loads of vacuum and seismic accelerations or of the thin-bladed flexures. Such non-linear failure scenarios are being mitigated with conservative analysis and component qualification test programs to ensure all such structural components have large margins of safety.

Finally, accidental overpressure of the cryostat during venting could result in damage to an O-ring seal, feedthrough, or failure of the vacuum vessel itself. This is being addressed by designing the Cryostat to carry overpressure loads, over-pressure proof-testing it, then also providing a burst disk to ensure that an over-pressure cannot exceed this limit.

10.5.3.4. Electrical

Thermal components within the Cryostat have heaters and temperature sensors mounted to them. The heaters, in particular, could fail by shorting across elements or to ground, causing sudden sharp rises in current. Such hazards will be managed by the control system for the heaters, which will include over-current protection and current monitoring to ensure that heater circuits shut off if such a short occurred.

10.5.3.5. Control

The Cryostat contains elements of thermal, vacuum, and power systems which rely on the functioning of each other and of elements outside the Cryostat. Many of these functions are commandable from the control system, as well. Loss of control, operator error, or failure of one component could produce a more significant problem or failure elsewhere in the system. These hazards are mitigated by implementing enable/disable control for functions handled by a single controller. For those that bridge between controllers or outside of the cryostat, functional interdependencies are monitored and actions allowed/disallowed by the camera protection system. This will ensure that prevented actions that could damage another subsystem are disabled.

10.5.3.6. Environmental

When the Cryostat is not cold, it will be vented and at atmospheric pressure. Since any contaminant in the Cryostat can migrate to—and possibly damage—the detectors, the Cryostat will always be vented with clean and dry nitrogen gas. However, when personnel are working on the Cryostat, we will use flow restrictors and possibly oxygen-deficiency monitors to detect any build-up of this asphyxiant and reduce the risk to personnel.

10.5.3.7. Fire

The refrigerant used in the Cryo and Cold Plate cooling channels is not combustible but in a fire their combustion products can be toxic to personnel. Inside the cryostat, these materials are fully contained in their channels, and in the event of a leak, there are no ignition sources within the cryostat and the nitrogen purge reduces the possibility of combustion. Outside the cryostat, the refrigerants may pose other hazards—for a discussion of these see Section10.6.3.

10.5.3.8. Materials and Substances

In the event of a release of the refrigerant used in the Cryo and Cold Plate cooling channels into the cryostat, it may be harmful to the CCD detectors and severely impact the cleanliness of the Cryostat. Risk of release of refrigerant in the Cryostat vacuum is being reduced by designing all fluid-vacuum joints with a double-seal. This includes two separate brazed joints with an intermediate pump-out that is monitored.

10.6. Refrigeration System

10.6.1. Functional Description

The refrigeration systems for the Camera provide cooling capacity to remove heat from components in the Cryostat and maintain them at stable cryogenic temperatures. The Cryo Plate refrigeration system supplies refrigerant to the Cryo Plate to hold the detector array on the focal plane at its -100 ^{o}C operating temperature and remove the combined load of infrared heating through the L3 lens and heat dissipated by the front-end electronics. The Cold Plate refrigeration system supports the Cold Plate, holding the Raft Control Crate electronics at their operating temperature of -40 ^{o}C. The two systems use similar technologies and design to achieve their function.

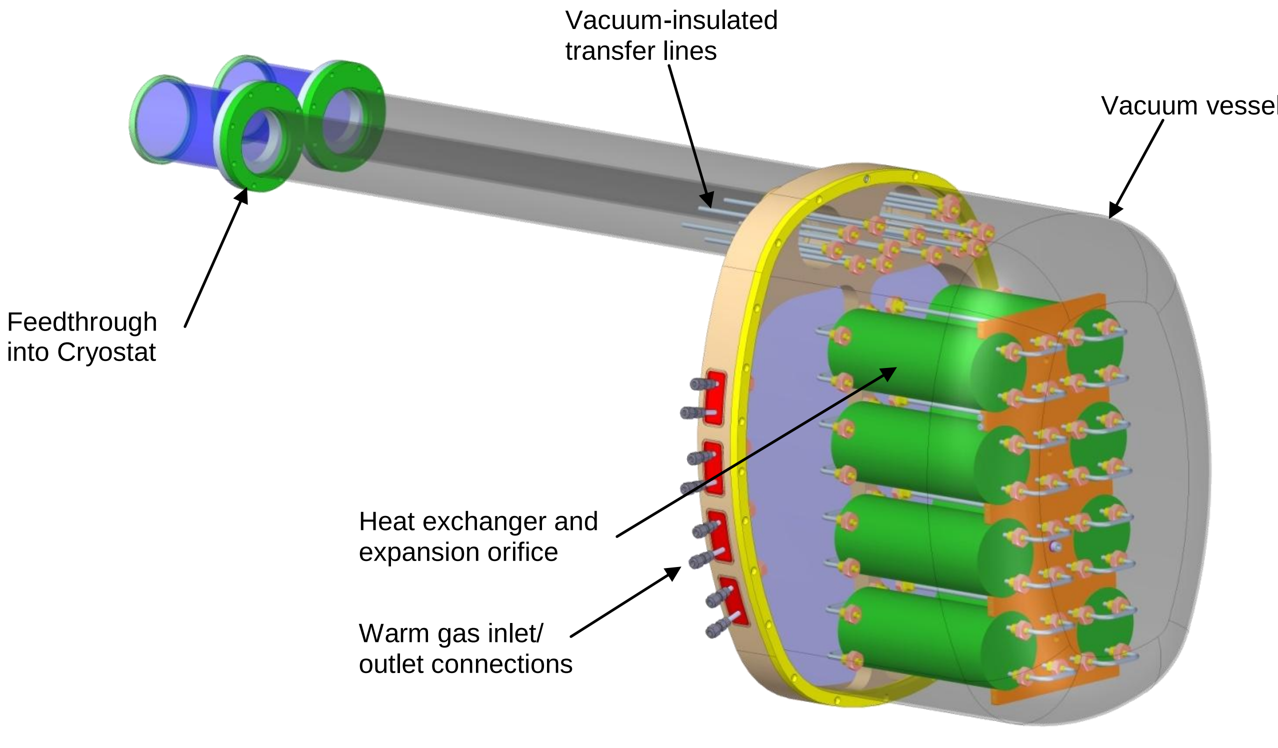


Figure 10: Refrigeration System Heat Exchanger in Utility Trunk

The refrigeration systems are based on a refrigeration cycle similar to domestic kitchen refrigerators. The Cryo Plate system reaches cryogenic temperatures by using a proprietary mixture of common chloro-fluoro-carbon refrigerants plus argon and nitrogen. The Cold Plate system is identical, except it uses only one refrigerant in its system.

Unlike a standard refrigerator, each system is divided into three geographically separate units. On the ground, the compressor, after-cooler, and oil separators supply high pressure refrigerant to room-temperature supply lines running up the telescope and across the three rotating degrees of freedom of the telescope. Once on the camera, the counter-flow heat exchangers in the Utility Trunk pre-cool the incoming refrigerant, which then runs through an orifice where it undergoes near-adiabatic expansion and cooling to its working temperature of -130 ^{o}C. From the vacuum-insulated heat exchanger, the now-cold refrigerant runs through cold supply lines into the cryostat, then into the Cryo Plate where it boils as it absorbs the process heat from the front end electronics. The liquid/gas mixture then flows back to the heat exchanger, is warmed up by the incoming refrigerant, then returns down the telescope in room temperature, low-pressure lines to the compressor.

10.6.2. Physical Description

The Cryo Plate refrigeration system reaches cryogenic temperatures by using a mixture of common non-flammable chloro-fluoro-carbon refrigerants plus argon and nitrogen. On the ground, a commercial 23 atmosphere hermetic reciprocating compressor with water-cooled after-cooler and oil separators is located in the camera utility room. Standard, off-the-shelf commercial hermetic compressors are used for reliability, which limits the size of an individual circuit to 120 watts at -130 ^{o}C. A cluster of six identical, independent refrigeration units is used to carry the full heat load off the Cryo Plate. Two additional parallel units are used for removing 400 watts from the Cold Plate at -40 ^{o}C using standard R507 refrigerant. Refrigeration capacity is controlled by variable speed compressors, while the temperature across the Cryo and Cold Plates is stabilized using electrical trim heaters. For long term reliability, the cold regions of the system are protected from plugging with frozen lubricating oil by an oil separator based on fractional distillation.

The ground facilities are completed with vacuum pump and purge systems and filling tanks to re-charge any given circuit, plus valves and instrumentation to monitor the system. Room-temperature supply and return lines couple the compressors in the utility room to the heat exchanger canister in the Utility Trunk on the camera. These lines are all solid metal brazed or welded lines except where they cross the rotating joints of the telescope. In these three locations, flexible hose is used to provide the compliance necessary to accommodate the large rotations of the telescope.

The vacuum-insulated heat exchanger canister contains counter-flow heat-exchangers and expansion capillaries. Each of the parallel circuits contains one of each. The heat exchanger pre-cools the incoming high-pressure gas using the outgoing cold gas/liquid combination that is re-heated in the process. Pre-cooled gas then flows through a long, small-diameter capillary where it cools by adiabatic expansion, liquefying in the process. Both the heat exchangers and orifices are wrapped in a tight coil which is warm at one end and very cold at the other. The coils are mounted in the heat exchanger canister, where they are in an insulating vacuum that is physically separated from the Cryostat vacuum. Supply and return transfer lines then plumb the cold liquid through vacuum-insulated tubes to the Feedthrough Plate on the back of the Cryostat. Here, the lines are brazed into a custom vacuum feedthrough and ground isolation break. The feedthrough separates the canister vacuum from that of the Cryostat, while the ceramic break in the lines allows for complete ground isolation of the entire cold mass in the Cryostat, thereby reducing the possibility of ground loops in the sensitive analog electronics.

Inside the Cryostat, the refrigeration lines are routed to channels in the Cryo and Cold Plate. All refrigerant-vacuum connections and joints in these lines and fittings are backed up with a vacuum guard region to reduce the possibility of refrigerant leaking through a bad connection and contaminating the Cryostat vacuum. These isolation volumes are pumped down with a separate vacuum system and monitored, so a leak can be detected as soon as it occurs.

Once through the Cryo and Cold Plates, the low pressure refrigerant then returns to the compressor through the low temperature counter-flow heat exchanger in the heat exchanger canister, where it is warmed back up to room temperature, then back down the telescope to the Utility Room.

10.6.3. Hazard Description

10.6.3.1. Thermal and Cryogenic

Given that the refrigeration systems' primary function is to cool components, one of the primary classes of hazards associated with the systems is overcooling or uncontrolled cooling. First, overcooling could occur if the heat source at the electronics in the cryostat is removed. This could happen due to either a planned turn-off or unplanned shut-down of the systems. In either case, the refrigeration system could provide far more cooling capacity than needed, which could cool down components inside the cryostat too much, or cool down the return lines, creating condensation and ice build-up. Both symptoms of overcooling are addressed by two mitigators. First, the refrigeration cycle has an inherent temperature floor, below which it cannot function, which is established by the peak pressure and the refrigerants being used. All hardware in the system is survival tested to this limit, to ensure that it can tolerate exposure to these temperatures. Furthermore, temperature sensors are used both for fine control of the system and for monitoring health and safety of the system. If the lines were to cool down beyond their preset limits, the system would shut down.

Another possible source of overcooling is the loss of vacuum in the heat exchanger canister. This could produce icing of the heat exchanger coils. While this is not preferred and would require recovery effort to repair the leak, this would likely not damage the heat exchangers. Furthermore, the possibility of a leak is mitigated by pressure and leak testing of the vacuum vessel, as well as monitoring of the vacuum pressure during operation. Sudden, catastrophic leaks in well-sealed all-metal vacuum vessels is not common, and any incipient leak is detected by upward trends of the vacuum pressure.

10.6.3.2. Pressure/Vacuum

The refrigeration systems are under high pressure and rely on large changes in pressure of the working gas to remove heat from the camera. Thus, over-pressurization is a hazard within the system. There are three possible causes for such a hazard, located along different points of the circuit. First, in the utility room at the compressor, if a valve were inadvertently closed, the compressor could overpressurize the ground circuit of the inlet lines. Up in the heat exchanger canister, a similar situation could be produced if the free-expansion orifice were to get plugged with frozen oil. In either case, the inlet line pressure would increase. Three controls mitigate this risk. First, the compressor includes overpressure shut-off capability to ensure it is not damaged. Second, the lines include burst disks as a last resort. Also, all lines and fittings in the circuit are rated and proof tested to beyond the maximum operating pressure, set by the relief pressure of the burst disk.

A similar overpressure scenario could occur on the low-pressure return line, due to a pinch in a line or valve closure. Here, also, relief valves and pressure-tested lines ensure that any overpressure is accommodated. Even though the return lines nominally operate at a lower pressure, they are rated and tested to the same level as the supply lines. This ensures that the entire circuit is pressure-rated to the same maximum operating pressure.

A different type of overpressure could occur in the heat exchange canister, if a high-pressure heat exchanger developed a leak. Here, the normally-evacuated heat exchanger canister would fill with refrigerant until it equalized in pressure with the high-pressure inlet line. This pressure is much more than the vacuum vessel typically handles. Such a scenario is addressed first by the vacuum pump on the canister, which would pump out any refrigerant from a small leak. Larger leaks would be handled by an over-pressure burst disk in the canister, which could accommodate the mass flow of the largest design leak in a heat exchanger.

10.6.3.3. Fire

Some common refrigerants are flammable. This is considered a significant risk, so it is being eliminated by designing the systems to use non-flammable refrigerants only. None of the constituents of the refrigerant mixture are flammable or explosive, so this hazard is eliminated.

10.6.3.4. Materials and Substances

The second hazard associated with a fire is that if a fire were to occur, the fumes and combustion products from the burning refrigerant are harmful to human health and the environment. This is a known hazard for the refrigerants in the systems. This is addressed in three ways. First, fire due to overheating in the refrigeration system itself is mitigated by monitoring the temperature of the compressors in the utility room. Second, sprinklers or another automatic fire-suppression system will be used in the utility room. Third, emergency procedures for the dome and support building will include provisions for the possible presence of hazardous fumes.

Apart from a fire, an accidental release of refrigerant in the Utility Room may pose a risk of asphyxiation. While the refrigerant mixture is at room temperature while in the room, it is under pressure and some of the constituents are heavier than air. A release in the closed volume of the room may displace air. This potential hazard is being addressed as the system is being developed and sized. If the volume of refrigerant is large enough to pose a hazard, the room may need to be outfitted with an oxygen-deficiency monitor or auxiliary ventilation system.

10.6.3.5. Contamination

There are three possible sites for contamination in the observatory: the CCD’s, the L3 lens in the Cryostat, and the mirrors in the telescope. Within the Cryostat, the risk of contamination due to inadvertent leak of refrigerant is reduced by adding secondary containment in the form of vacuum guards around every joint in the cryostat vacuum. This includes all welded and brazed connections, as well as mechanical fittings. The secondary containment volume is under vacuum and monitored continuously, and can be actively pumped if needed, so any small leak is quickly detected and can be addressed immediately.

In the Utility Trunk, a leak in a hose or tube fitting could release gaseous refrigerant into the air where it could contaminate the surface of the M2 mirror which surrounds the camera. This is mitigated first by pressure-testing the entire system prior to use. Also, all constituents in the refrigerant mix are benign and not expected to affect the mirror coating or substrate.

10.7. Science Raft Towers

10.7.1. Functional Description

Science Raft Towers are the modular building blocks at the core of the camera. Each of the 21 Science Raft Towers that form the focal plane of the camera is an autonomous, fully testable and serviceable camera capable of acquiring 144-Mpixel images in 2 seconds. It occupies a volume of about 13 x 13 x 28 cm^3 and dissipates over 25 W of power during readout, and consist of three major assemblies.

Raft-Sensor Assemblies (RSA) are a 3 x 3 mosaic of science CCD's that capture and convert incoming light to an electrical signal that is read out and reconstructed into an image. The mosaic of CCD's is held very flat on the focal plane of the telescope, to ensure that images are focused. The CCD's and entire raft tower are cooled to -100 ^oC to reduce dark current from the CCD's, while still providing good quantum efficiency in the near-infrared wavelengths.

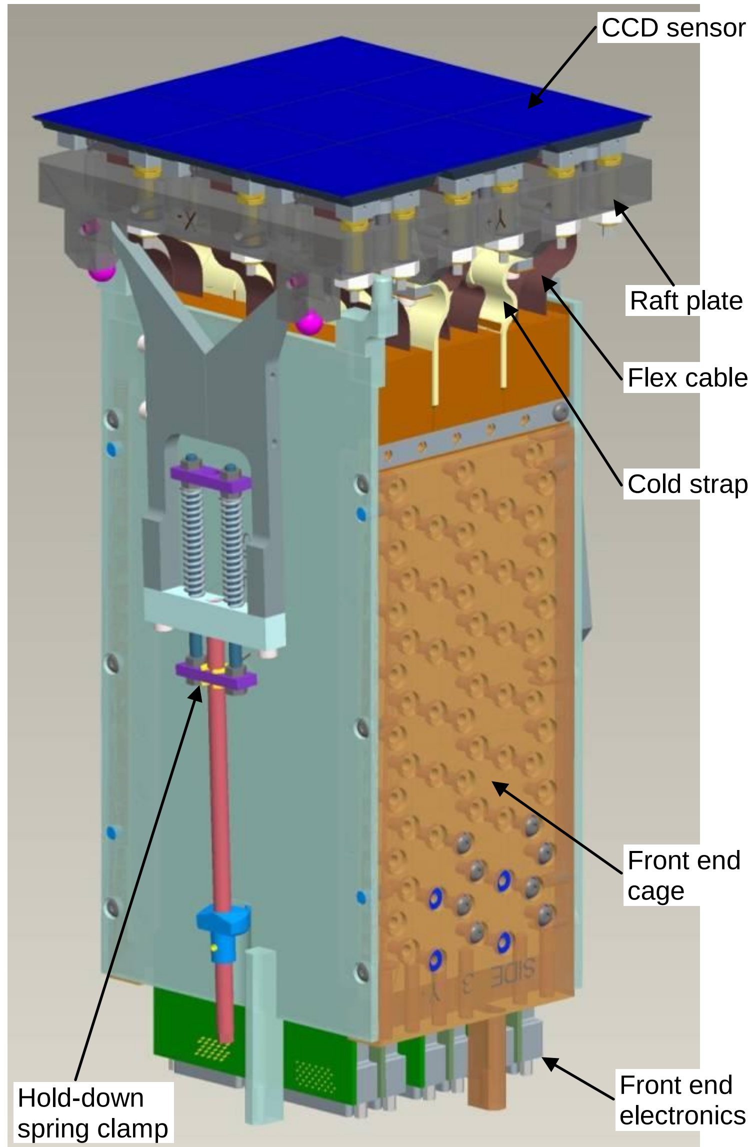


Figure 11: Science Raft Tower and Raft Control Module

The Front-End Cage (FEC) houses circuit boards to provide the correct bias voltages for the CCD's, collect and process the low-level analog signals from the CCD's, and provide synchronized timing pulses for the read-out of the CCD's. The FEC is packaged within the square footprint of the raft assembly to maximize the packing fraction of the CCD's on the focal plane.

The Raft Control Crate (RCC) contains electronics for digitizing the signal from the front end electronics and providing clock sequencing, bias generation, temperature sensing, and interfacing to the control and data acquisition systems. The RCC is also packaged within the footprint of the raft, and is maintained at -40 ^oC to reduce outgassing of the electronics components in the insulating vacuum of the cryostat that contains the raft tower and CCD's.

10.7.2. Physical Description

The Camera Cryostat contains 21 identical Science Raft Towers. Each contains 9 CCD sensors mounted to a flat silicon carbide baseplate using three precision studs to achieve a coplanar surface, along with two close-fitting alignment pins to locate the CCD's laterally. The CCD's are cooled by conduction through their mounting studs to the raft baseplate. The raft baseplate in turn is cooled by flexible thermal straps which connect to thick copper planes in the FEC; and are in turn bolted to the copper Cryo Plate heat sink Thermal sensors on each CCD and in several locations on the raft baseplate and front end boards provide temperature monitoring, and makeup heater resistors mounted on the raft baseplate are used to maintain stable temperatures on the CCD.

The underside of the raft baseplate has three precision vee-grooves which provide a kinematic coupling to spheres mounted on the Grid structure. The rafts are held to the Grid with spring-loaded arms that maintain a constant pretension on the kinematic couplings when the raft towers are integrated into the Grid. Electrical and thermal connections between the RSA and FEC are all compliant to allow relative motion between them and the raft during cooldown and to avoid applying bending moments to the rafts.

All front-end electronic functions are implemented as compact, ASIC-based circuit boards housed in the FEC and RCC. Each CCD is connected to a pair of Front End Boards (FEB's) by two flex cables with video, clock, and bias signals for eight amplifier segments. FEB's perform video signal processing and clock and bias analog buffering. Parallel and serial clocks are handled on alternate FEB's, and the parallel clocks are bussed across the CCD multilayer ceramic. The six FEB's are packaged in pairs with one providing the parallel clocks and half the serial clocks, and its mate providing the remaining serial clocks. They include heavy copper ground planes, thermal via's and edge plating regions which are clamped at the board edges and bolted to the FEC thermal planes. This provides an efficient conduction path with multiply-redundant heat transfer across all joints, to remove the heat generated on the board to the base of the FEC, while also providing an independent heat path for cooling the CCD's.

Boards in the RCC contain analog-to-digital converters, FPGA-based clock sequencers, buffer memory, and a high-speed serial interface to the science data acquisition system. The RCC is also responsible for generating CCD bias voltages, reading temperature sensors, and providing current to makeup heaters in the tower. The RCC operates at a warmer temperature, around -40 ^{o}C, to reduce the load on the cooling system and to allow the use of standard commercial electronics, while still reducing the rate of outgassing of volatiles off the electronic components. Back-end boards in the RCC's are mounted and thermally sinked to a copper crate which in turn is mounted to the Cold Plate. The boards are electrically connected to the front end boards by 12 flexible circuit boards—two per front end board—that span the gap between modules, fold up during integration of the RCC, but are long enough to allow for integration and reduce heat conduction down them.

10.7.3. Hazard Description

10.7.3.1. Thermal and Cryogenic

The SRT and RCC modules are designed to operate at very low working temperatures. However, as with any such system, the hardware can be damaged if the safe operating temperature range is exceeded either on the cold end or hot side. For the science rafts, over-cooling or rapid cooling could damage either the circuit boards due to larger-than-expected thermal stresses, or the detectors themselves. These risks are mitigated by the design of the refrigeration systems, which have an operational floor based on the thermodynamics of the working fluids. Also, the raft tower test program includes qualification and acceptance tests that cover the full survival temperature range of the system, to ensure that all raft towers can, indeed, endure the full range of temperatures that could be experienced. Furthermore, qualification tests demonstrate that the raft tower is capable of surviving a much larger number of temperature cycles than will be experienced in the planned operating life of the Camera.

On the hot side, sensors or boards could overheat during bench testing of components during integration. Here, mechanical failure is not possible, since components are all designed to endure much larger temperature gradients on the cold side. The most sensitive part of the assembly on the high temperature side is the Parlene C passivation coating which is damaged by extended exposure to temperatures over 80 degC. All Cryostat bake-out steps will be carefully controlled and monitored to ensure that maximum temperatures are not exceeded.

10.7.3.2. Structural

The raft tower is a relatively benign structural assembly, with low loads and high margins of safety. Most components are sized to maximize thermal conductivity, including the bolted joints in the assembly, thus mounting points are multiply-redundant and significantly overdesigned for carrying the structural loads. Two parts pose the most significant structural hazards of the assembly. The loaded rafts are held on their kinematic balls by three pre-loaded springs, to ensure that the loads and deflections are unchanging. However, failure of a spring or support feature would release the raft, causing it to drop out of its ball sockets and either hit the L3 lens or more likely to swing down and damage sensors in neighboring rafts, both of which would cause significant damage to the camera. This significant risk element for a single-point failure item is being mitigated on three fronts. First, the design of the spring mechanisms is fail-safe to the loss of a spring. The spring itself is a compression spring, which is fully contained and guided to eliminate any possibility of buckling or loss of compression. The support feature that holds the spring units to the Grid has also been designed to ensure that it is always fully engaged. Second, the system is designed with relatively high margins of safety on all components. Finally, the design is being prototyped and strength qualification tested to determine safe working loads, then production units will be proof-tested prior to use.

The second hazard risk associated with the structural design are the machined ceramic components that support the CCD sensors. Silicon-carbide ceramic is used for these to maximize heat conductivity and reduce thermal contraction of the assembly. However, the ceramic is more brittle than most metals and typically fails by fracturing, not yielding. The ceramic components are designed to minimize stress concentrations and sharp corners where chipping may occur, and installation tooling prevents collision of adjacent ceramic parts. A design option under consideration is the use of threaded ceramic differential screws for height adjustment. While three screws are used to position and support each sensor, only two are needed to support it, so the screws are redundant structures. Failure of one screw would not result in loss of a sensor, but would likely result in its misalignment only, and possible particulate generation. The likelihood of such a hazard is being reduced by prototype testing to ensure that the screw can carry not just the expected support and thermal contraction loads, but also those associated with misalignment and adjustment forces. Also, a more fracture-tough ceramic is being used to reduce the likelihood of a failure of the material.

The SRT assemblies include hundreds of threaded fasteners and thousands of surface-mount electronic components. Due to the sensor-down orientation of the tower in operation, components which become free due to thermal cycling could fall onto the underside of a CCD, possibly causing mechanical breakage or electrical shorting. The design incorporates conformal coating of the circuit boards, a conductance barrier between the FEC and RSA, and captive hardware where possible to mitigate this risk. Thermal cycling tests with dummy assemblies also address the likelihood of such an occurrence.

10.7.3.3. Electrical

The sensor read-out and digitizing electronics includes low-voltage power conditioning, clocking, and signal processing. As with any electronics system the two most common hazards are over-current or short-circuits and over-voltage due to power supply failure or electro-static discharge (ESD). Over-current protection is built into the circuitry of the power supply design and the design is intentionally divided into independent one-raft units of low total power, so this hazard is addressed at the source in the circuit designs. ESD hazards are the more serious of the hazards. This is mitigated by locating over-voltage protection diodes at all sensitive nodes where this is possible, and by administrative controls for handling of all devices including low-voltage circuits. This includes standards for packaging for storage and delivery of components, design criteria for test benches and clean room materials, and protocols for handling and testing of ESD-sensitive parts. While only a few components in the raft tower are ESD-sensitive, the entire Cryostat assembly will be treated with ESD precautions.

10.7.3.4. Contamination

The primary contamination risk for raft towers is contamination of the sensors by materials outgassing inside the cryostat vacuum. Such an event could significantly affect the response of the CCD sensors and possibly irrevocably damage them, making this a significant hazard. Raft towers include three possible sources of contamination for the CCD’s: outgassing of component materials, release of contaminants due to catastrophic failure of an electrical component, and inadvertent introduction of contamination during processing of assemblies.

Contamination due to materials outgassing is being addressed at the source with a materials and part characterization test facility. This is intended to test every material that is used in the cryostat to determine the quantity of outgassing and constituent materials being deposited, then also to assess the effect of deposited material on the system throughput. During production, this will be expanded to include component-level testing of all assemblies, both to qualify the assembly and test processes, and for a final acceptance test prior to delivery. Furthermore, getter canisters are installed in the Cryostat vacuum to trap some fraction of condensable contaminants. Also, components in the Cryostat are cooled down and warmed-up in a prescribed sequence to ensure that surfaces colder than the sensors provide cryo-pumping of contaminants away from the sensors.

The materials test facility will also be used to investigate materials released in a catastrophic failure of an electronic component. This hazard will also be mitigated by careful parts selection and derating of parts to increase design margins of safety.

The most likely source of contamination is cross-contamination of parts during processing, assembly, or testing. This source is addressed by process controls invoked by the camera contamination control plan (CCP), that defines clean room facility requirements, handling protocols, and cleaning procedures for all components being used in the camera. This will reduce the likelihood of cross-contamination, then final assembly acceptance tests will still be used for a final check before components are integrated into the cryostat.

10.8. Corner Raft Towers

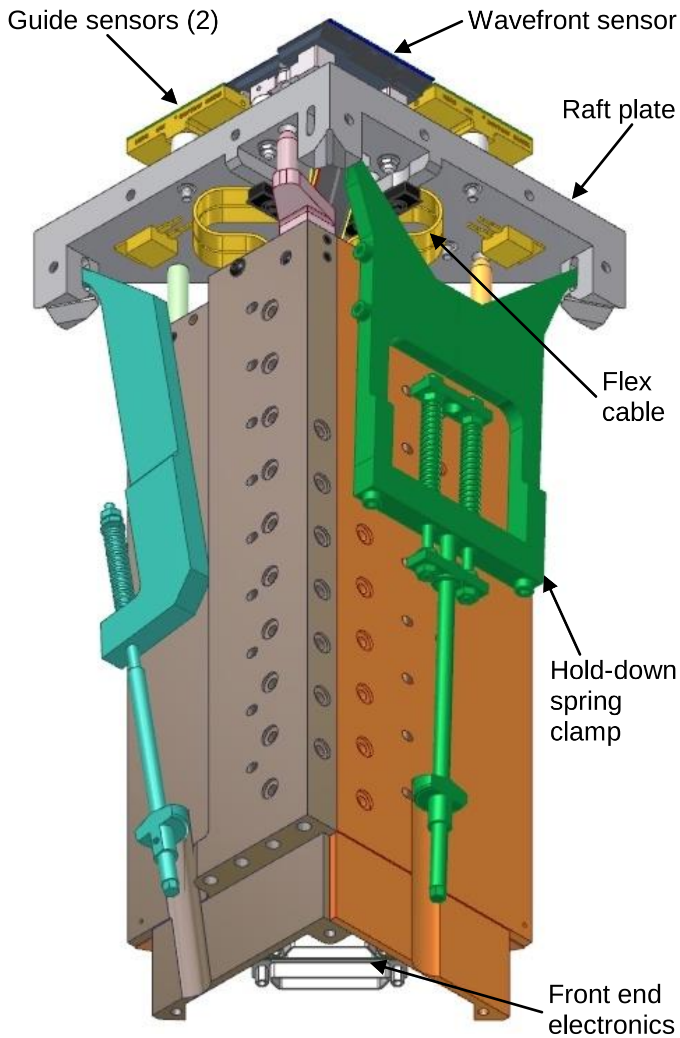


Figure 12: Corner Raft Tower

10.8.1. Functional Description

Corner Raft Towers, as the name implies, are located at the four corners of the focal plane, inside the Cryostat. The triangular rafts contain one wavefront sensor and two guide sensors, each, while front-end electronics for them are packaged within the footprint of the triangular raft behind the focal plane. The raft operates at a nominal temperature of -100 ^{o}C, the Front End Module slightly cooler than that, and the Raft Control Module at -40 ^{o}C.

The corner raft wavefront sensors acquire pixel data for the observatory active optics system based on curvature wavefront sensing. To support this activity, the corner rafts acquire intra- and extra-focal images from sensors 1 mm above and below the focal plane at 4 locations around the periphery of the focal plane. These images are used by the Telescope Control System to estimate the wavefront and, through reconstruction, provide inputs to the active optics controller. Images are collected in parallel with the science images and follow the corresponding exposure time and cadence.

The corner raft guide sensors acquire small images centered on selected bright stars at a nominal 9 Hz rate. These images are used to estimate the changes to the pointing of the telescope during an exposure due to wind buffeting, vibration, or slight inaccuracies of the telescope tracking. These changes are then provided as feedback to the telescope tracking system.

10.8.2. Physical Description

The Camera cryostat contains four sets of guide sensors and wavefront sensors in corner rafts at the edge of the camera FOV. Each Corner Raft Tower contains one wavefront sensor and two guide sensors and dedicated front end electronics for those sensors. The mechanical and thermal design of the corner rafts is as similar as possible to the science rafts.

Front-end electronics for operating the wavefront and guide sensors are packaged within the volume behind the detectors, similar to the science raft configuration, in an electronics crate. The Grid supports as little mass as possible—only the sensor rafts and their supports—to reduce gravity induced deflections. The tower is supported and cooled by the Cryo Plate at -130 ^{o}C. Each corner raft is thermally connected, but structurally decoupled from the tower by use of copper thermal straps to remove the electrical and radiant heat load from the Corner Raft and conduct it back to the Cryo Plate. Electrical connections between sensors and front-end electronics boards are made by flat flex circuit cables.

Back end electronics for operating the wavefront and guide sensors are packaged within the volume behind the corner raft towers in the RCC's. The control crates are supported and cooled by the Cold Plate at about -40 ^{o}C. The cold plate removes process heat from the power, clock, and digital back end electronics. Flat flex cables are used to make the electrical connections between front end electronics boards in the tower and back end electronics boards in the control crates.

Each of the guide and wavefront sensor packages are mounted to the corner raft plate structure by means of 3 threaded stud/pin legs, Belleville washers and locking nuts. Removable, thermally-conductive spacer/shims that can be adjusted are used to set the height of the sensor surfaces above the corner raft. Identical corner rafts are mounted in four corner locations on the grid structure (which also supports the science rafts) by means of an adjustable 3-point ball-and-vee kinematic mount design. The vees uniquely define the position of the corner raft with respect to silicon-nitride ceramic balls that are fixed in cups mounted on the Grid. This forms a kinematic connection that isolates the rafts from Grid distortion due to external dynamic and transient loads, assembly tolerances, and to the expected thermal motions due to differential contraction during cooling. The corner rafts are held in position by springs that pre-load the corner rafts against their kinematic coupling to the Grid, producing a uniform, invariant loading. The deflection of Grid and corner raft due to the spring loading is compensated for during initial integration, and remains unchanged in operation, independent of camera orientation and temperature.

10.8.3. Hazard Description

Hazard risks in the corner raft towers are identical to those in the science raft towers, given their very similar design. For completeness, they are repeated here in brief. See Section 10.7.3 for a more detailed description.

10.8.3.1. Thermal and Cryogenic

The corner raft tower and raft control module can be damaged if the safe operating temperature range is exceeded either on the cold end or hot side. These risks are mitigated by the design of the refrigeration systems, and acceptance test program for the corner raft towers.

On the hot side, out-of-range test conditions will be mitigated with test procedures and instrumentation to monitor the test and ensure that maximum temperatures are not exceeded.

10.8.3.2. Structural

The corner raft tower is held with a spring support system identical to the science rafts. Failure of a spring or support feature would release the raft, causing it to drop out of its ball sockets and either hit the L3 lens or damage sensors. The hazard is mitigated by the design of the spring mechanisms, relatively high margins of safety on all components, and a prototype and strength qualification test program, followed by proof-testing of production units.

The second hazard risk associated with the structural design is failure of one of the three redundant threaded ceramic differential screws that support the sensors. The likelihood of such a hazard is being reduced by prototype testing and use of a more fracture-tough ceramic, to reduce the likelihood of a failure of the material.

10.8.3.3. Electrical

The two most common electrical hazards are over-current or short-circuits and over-voltage from power supply failure or due to ESD. Over-current and over-voltage protection is built into the circuitry of the power supply design, so this hazard is addressed at the source in the circuit designs. ESD hazards are mitigated by administrative controls for handling of all devices including low-voltage circuits, including standards for packaging, design criteria for test benches and clean room materials, and protocols for handling and testing of ESD-sensitive parts.

10.8.3.4. Contamination

The primary contamination risk for raft towers is contamination of the sensors by materials outgassing inside the cryostat vacuum. Contamination is being addressed at the source with a materials and part characterization test facility, that will be expanded to include component-level testing of all assemblies. Cross-contamination is addressed by process controls invoked by the camera CCP, that defines clean room facility requirements, handling protocols, and cleaning procedures for all components being used in the camera.

10.9. System Electronics

10.9.1. Functional Description

Camera Support Electronics includes electronic components and systems that provide power, communication, and timing infrastructure for subsystem electronics devices. These reside mostly within the Camera Utility Trunk or Camera Body. They are divided into four categories: power systems; controls systems; data transmission; and cabling plant.

10.9.2. Physical Description

10.9.2.1. Power Systems

Power system hardware provides the filtered, conditioned power for all services on the camera, as well as a uniform camera ground. First, power enters the camera at a disconnect at the rear of the Utility Trunk as 3 Phase 240 V AC. This is a five wire connection with 3 phases, neutral, and safety ground. A standard commercial filter box is installed at that entrance point to remove possible high frequency disturbances.

Next, the AC power is converted to 24 V and 48 V DC for use in the various DC-DC converters that serve the science and utility loads, then is further converted by DC-DC converters to supply the science and corner RCC's with power at the needed voltages. One phase of the incoming AC power is used as single-phase 120 V AC for operating motors for the mechanisms, and separately converted to 24 V DC for other noisy uses such as heaters and solenoid actuators, as well as for motor and thermal controllers and monitoring hardware.

The power filtering, conversion, and regulaton components reside in one or more of the electronics crates in the Utility Trunk. The crates are designed and located to allow for the removal and replacement of boards while the Camera is mounted to the telescope. All parts of the power system are controlled and monitored by the Camera Control System (CCS) through one or more Ethernet connections.

10.9.2.2. Control Systems

The default platform for CCS hardware is PC104—an unspecified but fairly low end and low power processor capable of running a full standard distribution of Linux. Real-world interfaces are provided by adding on PC104 boards for sensing and controlling the various parts of the Camera. The PC104 systems for the Shutter and Filter Exchange systems are located in the Camera Body, while the remaining controllers are located in the Utility Trunk. Each controller is a separately replaceable object, and all connections are made to allow for straightforward removal and replacement. Controller form factor is custom to accommodate mechanical support and conductive thermal mounts for the PC104 hardware, while allowing for connections to the cable plant.

10.9.2.3. Data Transmission Hardware

High speed data to or from the Science Rafts is converted from electrical to optical and vice versa in custom-designed circuitry located in the Utility Trunk. The coaxial copper lines from the cryostat

Feedthrough Plate connect to fiber-driver cards to accommodate the high data rate in a tight form factor, while allowing for troubleshooting and replacement of cards if necessary. Then fiber optic cables carry the data out of the Utility Trunk and down the telescope to the camera data acquisition systems on the ground.

For standard instrumentation data and control signals, an Ethernet hub in the Utility Trunk provides communication to and from the CCS. The connections within the Camera use copper CAT6 cable, while connections to the Camera control system hardware on the ground use standard optical fiber.

10.9.2.4. Cabling Plant

The Camera cable plant is comprised of five classes of copper and fiber cabling. First, cables between the Science Rafts and the Utility Trunk crates penetrate the cryostat Feedthrough Plate, carrying high speed data, power, and control signals. Second, power and control signal cables interconnect the electronic crates in the Utility Trunk and connect to every controlled or monitored object in the Camera. Third, data fibers run between the fiber-driver cards and the rear of the Camera—and ultimately to the Science Data System (SDS) and CCS locations in the Observatory. Fourth, power cables run from the power entrance filter to the AC-DC converters, then additional power cables connect up with DC-DC converters for supplying power to the rafts. Fifth, networking cables connect component PC104 controllers to the network hub in the Utility Trunk then are converted to optical fiber and run down the telescope to the CCS. All of these cables, together make up the internal cable plant of the Camera. The external cable plant from the Camera to the Camera electronics on the ground consists of high speed and control fibers as well as the AC power line. The Camera Protection System may also require a small set of copper connections between the Camera and the Camera utilities areas.

10.9.3. Hazard Description

10.9.3.1. Thermal and Cryogenic

Any of the active devices, but especially the power systems, can be damaged or cause damage to nearby components if the cooling is not active while the systems are powered and they overheat. The time constants for damage from overheating are relatively long—on the order of tens of minutes—so that protective measures based on monitoring a rise in temperature would be fully effective. Outside the Cryostat there should be no mechanism for reducing temperatures to the point where damage might occur. Some of the power systems may have natural ways to incorporate local overheating protection, but in general devices will include control loops in the CCS to monitor temperatures and sequence power appropriately. Furthermore, device temperatures are also monitored by the Camera Protection System to back up the CCS. This provides a hardware over-temperature interlock to shut down any device that exceeds its allowed temperature limit.

10.9.3.2. Electrical

Component failures or shorts in active devices could result in over-current. To protect against that possibility, the power supply system not only monitors currents into the various loads but implements over-current and over-voltage protection for all loads. This provides first order but not complete protection against catastrophic failures in the loads.

Another possible source of shorts to ground or other potentials is the abrasion of cabling. To protect against such a possibility, the cable plant is protected in all areas where abrasion or rubbing could occur to prevent cut-through of or failure of the insulating materials to avoid shorts or breaks.

10.9.3.3. Fire

If the Utility Trunk volume is purged with air, some of the electronics objects may pose a fire hazard. However, the energy densities are relatively low, so this is not expected to be a significant hazard. To mitigate against this, board designs use fire retardant materials such as FR-4. Furthermore, the Camera Protection System includes some level of smoke detection within the Utility Trunk and Camera Body. We will investigate if further monitoring or active fire-suppression is needed, but expect that it is not.

10.10. Camera Body

10.10.1. Functional Description

The Camera Body is comprised of the outer housing and back flange of the Camera, and provides structural support for all Camera hardware. The back flange bolts to the telescope rotator and serves as the primary mechanical interface for the Camera. Both the Cryostat and Camera housing mount to the back flange, as well as the filter Carousel base. The Camera housing mounts to the flange and encloses the entire Camera volume. The L1-L2 Assembly mounts to the front end of the housing, as well as the Shutter and Auto Changer.

10.10.2. Physical Description

The aluminum back flange and outer housing provide key interface and support roles for most of the camera components. The back flange mounts to the telescope rotator around two bolt circles. The annular flange has a large central hole in it, through which the Cryostat is inserted into the Camera, and off of which the Cryostat is supported. The flange is flat in this inner region, but flares out to a triangular cross-section at its outer diameter, to stiffen the interface and reduce deflection. Cut-outs in the cross-section provide pockets for Carousel motors and for routing cables out of the Camera. The Camera housing mounts around the outer perimeter of the flange with another bolt circle and O-ring seal.

The housing fully encloses the backward two-thirds of the Camera volume. Cut-outs in the housing provide access to the inside of the Camera for maintenance, but the portholes are sealed off during normal operation. At the front end of the housing, a flange stiffens the free end and provides a structural mounting interface. Here, the struts that support the L1-L2 Assembly mount and can be adjusted. Also, the Shutter mounts off of two bosses and two flexures. The Auto Changer bolts and pins into a cut-out in the front end of the housing, adding stiffness to the housing and closing out the notch.

Finally, a gas-tight sealing skirt bridges between the front end of the housing and the L1/L2 Assembly support ring. This completes the hermetic seal of the camera volume to ensure that it remains clean and thermally stable.

10.10.3. Hazard Description

10.10.3.1. Structural

The Camera housing, sealing skirt, and L1-L2 Assembly form an enclosure that is pressurized at a very slight positive pressure. If this were over-pressurized, the structure would be stressed above its normal operating stresses. However, the viton sealing skirt will vent any excess pressure and we will use a pressure-relief valve to ensure that in all circumstances the pressure in the Camera volume never exceeds its limits.

Since the Camera housing and back flange provide the primary structural support for the Camera, there is a risk that over-stressing or failure of one structural element could result in large-scale damage or collapse. To mitigate this, we are designing the flange and housing with conservative margins even under extreme seismic loading conditions. Also, bolt circles are multiply-redundant to ensure that no single failure can endanger the Camera structure.

10.10.3.2. Environmental

The hermetic seals that make up the Camera volume ensure that Camera components and optics operate in a clean, low-humidity environment. However, failure of any one of these seals could result in the introduction of contaminants into the volume. Such a failure is mitigated by slightly over-pressuring the volume to ensure that any leaks that form result in a net outward flow. Also, instrumentation will monitor both the internal pressure and flow rate of purge gas, so a leak can be identified.

If dry nitrogen is used as the purge gas, the Camera volume will be oxygen-deficient and a hazard for personnel accessing the Camera for servicing. Here, oxygen-deficiency monitors and administrative controls will be used to reduce this risk.

11. Activity-Based Hazards and Personnel Safety

11.1. ES&H Plans for Camera Activities

11.1.1. PPA Policy

The LSST Camera project is managed by the SLAC Particle Physics and Astrophysics (PPA) Directorate. The PPA Directorate is committed to carrying out its scientific mission in a manner that provides the utmost protection for all workers, the public and the environment. It is the responsibility of all PPA line managers and workers—including those involved with the Camera project—to understand and implement both the SLAC institutional safety programs and PPA project-specific plans and procedures associated with their work activities. All LSST Camera collaborators that perform work at SLAC will be required to register as users and have an identified SLAC point-of-contact (POC) that is responsible for ensuring they understand and implement SLAC safety programs and procedures. Short-term visitors are restricted to green work, as described in Section 11.1.3, below.

11.1.2. Integrated Safety and Environmental Management Systems

The safety of LSST camera operations at SLAC is governed by the SLAC Integrated Safety and Environmental Management System (ISEMS). The elements of this system include the five core functions and the seven guiding principles, which are depicted in Figure 13, below. This is described in detail in [Ref 8], "SLAC Integrated Safety and Environmental Management System Description," available on-line at: *http://www-group.slac.stanford.edu/esh/general/isems*

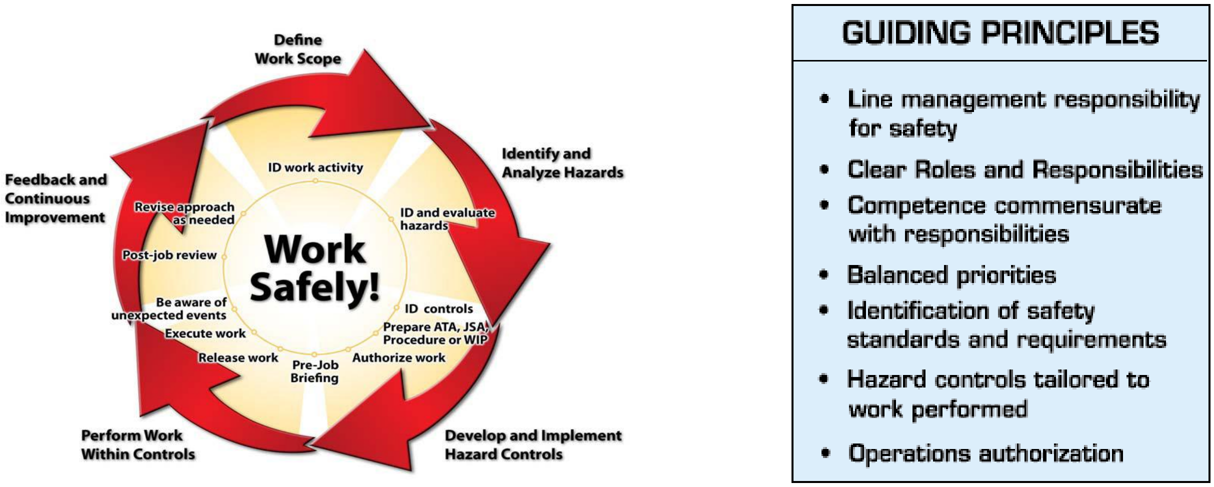


Figure 13: Five core functions and guiding principles of the Integrated Safety and Environmental Management System

Implementation of ISEMS is accomplished by applying multiple SLAC safety programs and processes. These include:

Work Planning and Control (WPC)
LSST Camera System Safety Engineering Program
Experimental Project Review Process
Subject Master Expert (SME) support
ES&H Division Support and oversight
ES&H Manual requirements and direction
Safety Training
Lessons Learned
DOE Stanford Site Office support and oversight

11.1.3. Work Planning and Control

The Work Planning and Control (WPC) process is an essential part of implementing ISEMS. Figure 13, above, contains in the interior the fundamental WPC steps and shows how they correlate to the ISEMS cycle. Categorizing, authorizing, and releasing work, as well as Work Integration Plan (WIP), Job Safety Analysis (JSA), Activity Training Assessment (ATA), Lessons Learned, and tailgate safety meetings, are some of the elements of this process. Requirements for—and implementation of—this process is described in [Ref 4], the SLAC ES&H Manual, Chapter 2, "Work Planning and Control," available on-line at: http://www-group.slac.stanford.edu/esh/general/wpc/policies.htm.

This WPC process will be used to manage work on Camera components through all phases of the project, starting with early development work and ending with final verification testing and delivery.

11.1.4. Experimental Project Review Process

The Experimental Project Review Process is described in the [Ref 4], the SLAC ES&H Manual, Chapter 1, "General Policy and Responsibilities," available on-line at: http://www-group.slac.stanford.edu/esh/general/general_policy/policies.htm.

This process is managed by the Safety Overview Committee (SOC), which will ultimately provide formal approval to operate specified equipment after review and approval by selected Subject Matter Experts (SME), Safety Officers, or other designated technical personnel. The SOC is composed of five core members (scientists or engineers) and seven *ex-officio* members that are listed below.

Radiation safety officer
Laser safety officer
Electrical safety officer
Fire marshal
Building Inspection Office lead
Environmental lead
Directorate ESH coordinators

Other technical specialists may be called upon to support the review of specific projects. These may include personnel with expertise associated with: pressure vessels, oxygen deficiency, unique experimental hazards, seismic, non-ionizing radiation, or other specialties as needed.

SOC involvement in the LSST Camera project has been initiated with an introduction to the Camera and its hazards by the Camera chief engineer and safety officer in early 2011.

11.1.5. Safety Training/Orientation

In addition to the SLAC-required training, the Camera project will develop specific camera safety orientations and training sessions for all for LSST Camera personnel both resident at SLAC and from collaborating institutions who will participate in any camera integration or test activity.

11.1.6. Oversight of Activities

Direct safety oversight of safety-critical activities will be managed by PPA Safety personnel. In addition, ES&H Division SME's will be called upon to provide guidance, support, and oversight as needed. The final level of safety oversight will be provided by the DOE Stanford Site Office.

11.2. Phases of Camera Construction

The LSST Camera project is divided into three distinct phases that span the life of the camera. Each phase presents some unique hazards to personnel based on the expected activities, but all share common classes of hazards based on the design of the Camera and activities expected to be performed.

The first phase of the Camera project involves the design and development of Camera components and subsystems. This includes building and testing engineering test units and prototypes to demonstrate a given technology, validate that a design functions as needed, or qualify a design under test conditions. In this phase, hardware and test set-ups are developed for the planned test and may or may not resemble the final implementation of the Camera design, although the test units always incorporate some aspect of the design's functionality.

In this phase, personnel and environmental safety is assured by following the WPC process described above. In particular, this includes specific planning for the test-specific operations that may differ from the final implementation. As with any WPC, this will be reviewed and approved prior to the start of work.

The second phase of the project involves fabrication, assembly, and test of camera components and sub-assemblies. This will be performed at a number of different locations among the collaboration, including at SLAC. Here, assembly and test plans will continue to follow the WPC process, with added emphasis on quality assurance and verification test planning. This process is essential to assure that the end product meets its requirements, as well as to ensure that all process steps can and are performed according to the WPC process.

The final phase of the Camera project is integration and test of the full Camera. This entire process will take place in Building 33 at SLAC, using hardware delivered from collaborators around the world. Here, additional hazards will be encountered due to the size and complexity of the fully-integrated system. This will require special attention to work planning to ensure that the work's impact and attendant hazards to personnel are addressed for all possible sources hazards, including systems apparently not directly affected. This, also, can be a time where unexpected events occur—such as components not fitting together or ground loops presenting problems with testing. Thus, contingent actions will need to be carefully controlled to assure that the affects and hazards associated are well-understood and we never rush into action without fully measuring and planning for the possible outcomes.

While each phase presents unique challenges and potential for hazards, all work on the Camera project at SLAC will be managed centrally and uniformly, to ensure that the ISEMS principles are incorporated into all aspects of the project.

11.3. Camera Activity-Based Hazards

11.3.1. Introduction

The hazards described in Chapter 10, above, focus exclusively on those that arise during standard operation of the camera in its installed configuration. These hazards include both those to the system and its constituent parts, as well as to personnel. However, they specifically do not address those hazards associated with the assembly of camera components or integration and test (I&T) of the camera prior to the start of operations. This chapter focuses specifically on the integration and test hazards. Instead of organizing this by subsystem, they are classified by type of hazard posed to personnel and the environment, describing both the extent of the hazard as well as the expected controls to assure a safe work environment.

11.3.2. Brittle Materials

11.3.2.1. Hazard Identification

The LSST Camera includes many components made from brittle materials that pose hazards to personnel working around them. In particular, the most significant hazard involves the large glass optics. These will be moved, stored, and ultimately lifted into place and mounted on the Camera during the integration process. During Camera verification testing, the L1 lens will be exposed to potential damage, and filters will be moved into and out of the camera. Throughout the I&T process the single largest hazard associated with these optical elements is a mishap that results in catastrophic failure of a lens or filter. Such a failure could result from dropping or loss of control of it during a lifting or moving operation, and could lead to shards of shattered glass spread throughout the area.

At a less severe but more plausible hazard level, the CCD detectors that form the detector plane are made from 100 micron thick silicon. These are also very brittle, and extremely fragile. Any kind of collision or rough contact with them would likely lead to a CCD cracking. While the CCD is bonded to its package, there is a possibility of small shards of silicon breaking off in the process.

The final hazard associated with brittle failure involves the use of either brittle or less fracture-tough materials as structural elements in the Camera. The silicon-carbide Grid is one such structure. While wholesale fracture of the Grid is extremely unlikely, a more plausible hazard involves local damage due to sharp impact with a tool or other hard object. Such an impact could lead to local fracture and brittle failure. The carbon fiber struts are the other structure that could fracture upon failure. While the epoxy matrix absorbs considerable energy in a high-energy impact, large-scale failure of a strut could result in cracked and frayed carbon fibers being exposed.

11.3.2.2. Hazard Controls

Brittle fracture and the resulting personnel hazards do not cleanly fall under one ES&H protection plan, so the hazards will be addressed on four fronts. First, at the design and design review levels, brittle fracture is being addressed directly by incorporating special safety factors as described in Ref [6], the "LSST Camera Environmental Specification." Depending on the component, these will also be designed and reviewed according to Ref [4], the SLAC ES&H Manual, Chapter 14, "Pressure, Vacuum, and Cryogenic Systems." Second, the lenses, filters, and structural elements will all be proof-tested to their respective proof pressure or loads. This ensures that there are no flaws that could lead to premature failure. Third, for the large optical elements, in particular, we will address adding covers to protect the elements during all handling, lifting, and integration steps. Besides the personnel hazard associated with these elements, they are very high-value components that must be safeguarded from any kind of damage. Protective covers will also serve to contain any shattered glass in the event of a catastrophic failure. Such secondary containments will further mitigate the hazard. Finally, appropriate PPE will also be used when personnel are exposed to these hazards. This could include the use of safety glasses, full face shields, or other protective equipment as appropriate. In defining the appropriate level of PPE we will use Ref [4], SLAC ES&H Manual, Chapter 19, "Personal Protective Equipment" and Chapter 5, "Industrial Hygiene."

11.3.3. Cryogenics

11.3.3.1. Hazard Identification

The Cryostat contains a cryogenic refrigeration system to cool the CCD sensors. The system uses a mixture of refrigerants and inert gases to produce temperatures down to -135 ^{o}C. This system operates at the warm end of traditional cryogenic systems, and does not use any liquid cryogens (nitrogen, argon, oxygen, or others). There are three types of personnel hazards associated with working on and around this system. First, the mixed refrigerant supply is under pressures up to 350 psi, introducing hazards associated with any high-pressure system, such as leaking, bursting, over-temperature of the compressor, and other system hazards. Second, when operating, the free expansion of the refrigerant will significantly cool it, allowing us to operate at our planned temperature. However, during testing of the system, cold surfaces could be exposed, causing frostbite hazards to personnel. Finally, in the event of a catastrophic failure to the system, refrigerant could be released into the room. While all of the constituents of the mixed refrigerant are benign both to personnel and the environment, they could pose an asphyxiation hazard if enough volume were released into a small room.

11.3.3.2. Hazard Controls

The Cryostat refrigeration system and associated cold mass will be designed according to Ref [4], the SLAC ES&H Manual, Chapter 14, "Pressure, Vacuum, and Cryogenic Systems." This will govern the design and test safety factors, test levels, and review and certification process. Furthermore, ancillary hazards associated with the use of compressed refrigerants will be addressed in Chapter 38, "Compressed Gases," and Chapter 36, "Cryogenic and Oxygen Deficiency Hazard Safety." This includes using oxygen-deficiency monitors in rooms where the refrigeration system is used.

11.3.4. Electrical

11.3.4.1. Hazard Identification

The LSST Camera uses a number of custom-built electrical and electronic systems. Most of the electronic systems operate at 48 V DC or less and thus do not pose any high-voltage hazard. However, a number of motors, actuators, and vacuum system components operate at high voltage or high current and pose hazards to personnel working around them while they are in a state of partial assembly or are being serviced. Furthermore, many of the Camera electronics systems are custom designed and not rated by any recognized agency to verify system safety. Thus, hazardous designs or unsafe implementations could lead to electrical shock.

11.3.4.2. Hazard Controls

Hazards associated with the custom electronic systems and high voltages will be addressed in accordance with Ref [4], the SLAC ES&H Manual, Chapter 8, "Electrical Safety." This will be used in the design and review of all such systems, as well as their operation and servicing.

While the Camera is not a facility, per se, it is a self-contained system. Thus, we plan to include a dedicated safety ground within the Camera and not rely on either incidental grounding to external structures or the neutral phase of our electrical feed line. The safety ground will be used during I&T, as well, to protect personnel working on the Camera. Similarly, we plan to include a "breaker panel" facsimile on the Camera to isolate electrical power from subsystems with lock-out/tag-out protection for personnel who need to access subsystem. This local protection will ensure that we have the flexibility needed for maintaining Camera subsystems, while ensuring that personnel are safe from electrical hazards.

11.3.5. <u>Hazardous Materials</u>

11.3.5.1. Hazard Identification

The Camera conceptual design does not include any materials known to be toxic or hazardous to the environment or personnel. During I&T, some hazardous materials will likely be used during the normal course of work. These include the use of ethanol and acetone as cleaning agents.

11.3.5.2. Hazard Controls

The use of alcohol and acetone cleaning agents will be controlled according to Ref [4], the SLAC ES&H Manual, Chapter 40, "Hazardous Materials." In particular, the storage, use, and disposal of them and any contaminated materials, will be handled according to the facility safety plans introduced in Section 11.4.3, below, and Ref [5], the "LSST Camera I&T Plan."

11.3.6. <u>Fire Safety</u>

11.3.6.1. Hazard Identification

During Camera I&T, no unusual fire hazards exist. Apart from the use of alcohol and acetone cleaning agents, the Camera does not use any flammable materials.

11.3.6.2. Hazard Controls

During Camera integration and test, we will use the fire detection and suppression systems already in use in the I&T facility at SLAC. These are in concordance with Ref [4], the SLAC ES&H Manual, Chapter 12, "Fire and Life Safety." See Section 11.4.5, below, for information about facility fire safety plans.

11.3.7. Hoisting, Rigging, and Support

11.3.7.1. Hazard Identification

There are three types of hazards associated with hoisting and rigging of camera components, as well as in the support of the camera and its major sub-assemblies during integration and test. First, facility and portable cranes and lifts will be used extensively for many conventional hoisting operations during I&T. All such lifts use standard rigging and lifting procedures, but nonetheless involve suspended loads in the presence of personnel.

Second, during camera I&T there will also be "non-conventional" lifts, which require special planning of some type for three possible reasons. A number of lifts involve the use of custom-designed below-the-hook lifting frames, spreader bars, or other attachments. This includes lifts of the Cryostat, L1-L2 Assembly, and the Camera as a whole, each of which include special frames for load distribution, balancing, or restricted hook height. Furthermore, some of the lifts involve loads approaching the rated load of the crane. While these are still considered safe loads, additional planning is warranted to assure that the lifts proceed as expected. Also, a few of the key lifts involving final integration of the Cryostat and L1-L2 Assembly into the camera involve large structures that take up a lot of volume relative to the volume of the crane hook envelope. Once again, there is nothing inherently hazardous about this, but it introduces complications, including blocked and incomplete sight-lines for riggers and operators, multiple points of approach, and limited-access regions for personnel around suspended loads.

Finally, a number of fixtures will be used to support and position camera sub-assemblies during the relatively long integration and test process. During Cryostat integration, the partially-integrated Cryostat will be moved between three such stands, one each for inserting Raft Towers, for measuring flatness of the detector plane, and for re-orienting the Cryostat and moving it around. During Camera integration, the Camera back flange and outer housing are supported off of a frame that pins to a support stand. This frame can be re-positioned to orient the Camera from zenith- to horizon-pointed during in-process testing. Safe design, fabrication, and use of these support frames is clearly important to ensure the safety of the hardware and personnel working around them.

11.3.7.2. Hazard Controls

All types of hoisting and rigging operations will be controlled pursuant to Ref [4], the SLAC ES&H Manual, Chapter 41, "Hoisting and Rigging." This includes establishing criteria for the design, review, and fabrication of under-the-hook lifting fixtures, crane and fixture certification testing, and planning for the lifts themselves.

Lift planning will be part of the overall work planning and control process, described in Ref [4], the SLAC ES&H Manual, Chapter 2, "Work Planning and Control." This process is further described in Ref [5], the "LSST Camera I&T Plan," where its implementation for Camera work at SLAC is delineated.

11.3.8. Ionizing Radiation

There are no planned sources of ionizing radiation used in the camera or during the I&T process. However, an iron-55 source may be used for verification testing, but is not yet baselined.,

11.3.9. Lasers

Lasers are not planned to be used in the camera or during the I&T process. However, they may be added as part of verification test plans, but are not yet baselined.

11.3.10. Oxygen-Deficiency

11.3.10.1. Hazard Identification

During integration and test, there are three sources of asphyxiants that could produce oxygen-deficient volumes in the facility. First, the refrigeration system contains considerable volumes of high pressure refrigerant that, in the event of a severed tube or fitting, would expand into the surrounding room. This is not expected to pool on the ground as conventional cold cryogens would do, so the primary hazard is associated with displacing the air volume in the room. Second, during integration, the Cryostat will be tested often by evacuating it then cooling it down for testing. When the test is completed, it will be warmed up, then the volume vented by backfilling it with dry nitrogen. This will be supplied by tubes from the facility nitrogen system. Any break in a supply tube or vent of nitrogen from the Cryostat proper would produce a very local low-oxygen environment around the Cryostat. Furthermore, the facility nitrogen purge system will also be used for purging components waiting for integration in dry cabinets in the clean rooms. Any break in a purge line would result in larger-than-expected flow of nitrogen in the clean room.

11.3.10.2. Hazard Controls

All low-oxygen hazards are controlled by the oxygen-deficiency monitoring system already existing in the facility clean rooms. This system is described in Section 11.4.2, and meets the operational requirements established in Ref [4], the SLAC ES&H Manual, Chapter 36, “Cryogenic and Oxygen Deficiency Hazard Safety.” . Furthermore, as the refrigeration system is finalized, further analysis will be performed to better understand any hazards associated with the sudden release of refrigerants into the enclosed clean room volume or utility room area in the high bay of Building 33. While there is a limited supply of refrigerant, it expands considerably, so we will investigate the total possible volume of a release and the capacity of the room ventilation system to remove the refrigerant.

11.3.11. Pinch and Crush

11.3.11.1. Hazard Identification

There are two sources for pinch and crush hazards associated with assembly and integration of the Camera. First, both the Shutter and Exchange System include mechanisms that can be remotely controlled to actuate them. For both systems, in all cases the actuation involves a single-degree of freedom motion at relatively low speeds. However, they pose a hazard to personnel working around them since the motions involve enough force to pinch or crush a finger if it were in the path of the actuation. Note that this hazard only exists when the camera and subsystems are open to personnel. During normal operation, mechanisms are not exposed to personnel.

The second source of crush hazard is during operation of moving support fixtures and hoisting Camera components. In both cases, the hazard involves personnel being trapped between a moving piece and fixed member. To a large extent, this hazard only exists for short time periods during specific lifting or moving operations, since we do not anticipate having any fixtures with powered degrees of freedom.

11.3.11.2. Hazard Controls

Pinch/crush hazards will be controlled in two ways. First, for the Shutter and Exchange system, most of the hazards are being mitigated in the design of the mechanisms. This is being done by adding passive safety guards and wipers to prevent entrapment of digits or clothing during operation. For the few remaining crush hazards, administrative controls will be invoked to assure personnel safety. These controls are expected to include the use of additional guards and safety devices during exposed testing, as well as lock-out/tag-out devices to ensure the removal of power during access. Such administrative controls will be pursuant to the requirements of Ref [4], the SLAC ES&H Manual, Chapter 51, “Control of Hazardous Energy.”

Hazards associated with movement of components during hoisting and movement of fixtures will also be controlled administratively, through careful work planning and control, clear procedures on the safe operation of fixtures, and lifting plans for all lifting operations.

11.3.12. <u>Pressure and Vacuum Vessels</u>

11.3.12.1. Hazard Identification

The Camera includes four pressure/vacuum systems: the Camera housing, Cryostat, Heat Exchanger Can, and refrigeration system. These systems are described in detail in earlier sections of this document, along with the hazards they pose both to personnel and other equipment. In summary, these hazards include over-pressurization and leak/rupture of a system, including during backfilling or purging, implosion of an evacuated vessel, and release of refrigerant through a failed fitting or burst line. These hazards exist both during normal operation as well as integration and testing. The added hazard during I&T is the presence of people, where a rupture—especially of one of the lenses forming part of the pressure envelope—could cause injury.

11.3.12.2. Hazard Controls

For all hazards related to pressure and vacuum systems, controls will be consistent with Ref [4], the SLAC ES&H Manual, Chapter 14, “Pressure, Vacuum, and Cryogenic Systems.” These controls include requirements for system and component design, review, fabrication, assembly, and test, as well as operation, so they will be included in the design of the system as it matures during the development phase. Some provisions have already been included in specifying maximum operating pressures and test pressures, as defined in Ref [6], the “Camera Environmental Specification,” as well as in the design of systems to include relief valves, burst disks, and overpressure switches.

11.3.13. Seismic

11.3.13.1. Hazard Identification

The Camera will be integrated, tested, and operated in seismically active regions of the world—at SLAC and in Chile—so seismic safety is imperative. Since the Camera is an inherently safe system, our primary seismic hazard is associated with seismic ground accelerations that lead to additional forces and accelerations being imparted on Camera components. During integration, an additional concern is imperilment of personnel working around Camera components during an earthquake. This is an issue both at SLAC and on the summit in Chile.

11.3.13.2. Hazard Controls

While the Camera is ultimately being installed on the summit in Chile, we plan to use Ref [7], "Seismic Design Specification for Buildings, Structures, Equipment, and Systems," to govern the design and installation of the Camera and all support fixtures both at SLAC and on the summit. Peak ground accelerations have been defined and are listed in Ref [6], the "LSST Camera Environmental Specification."

Since the integration and test process at SLAC spans multiple years, all integration stand and test configurations are being designed to meet the criteria established in Ref [7]. This include design factors of safety, review criteria, and installation and anchoring requirements.

11.4. Facility Safety Plans

11.4.1. Introduction

The LSST Camera will be integrated and tested in Building 33 at SLAC. Furthermore, some subsystem hardware will also be assembled and tested separately in the facility, prior to being integrated into the Camera. The existing facility includes many safety features to address typical hazards associated with such facilities. These safety systems are introduced in the following sections, and further detailed is included in current facility plans which will be updated for LSST Camera use.

11.4.2. Oxygen-Deficiency Monitoring

Building 33 clean rooms are equipped with boil-off nitrogen purge lines, which poses the primary oxygen-deficiency hazard in the facility. Oxygen-deficiency monitors (ODM's) are used in the clean rooms to warn personnel of reduced oxygen levels in any of the rooms. At least two oxygen sensors are located in each purge area. If any oxygen sensor in the building goes below 19.5% then an automatic shutoff valve closes and stops the flow of nitrogen to the facility and an alarm signal is automatically sent to the fire department. The facility nitrogen must be reset after an alarm has been triggered.

The maximum allowed purge rate for each room is set by requiring that even with complete loss of facility and ODM power, it takes at least 8 hours before the oxygen level in the room is reduced by 1%. Table 5 lists the approximate room volumes and allowed purge rates for each room. Note that this assumes perfectly sealed rooms, which is quite conservative, and that the nitrogen purge mixes completely with the room air. Since the nitrogen purge gas is delivered at room temperature, this is a safe assumption.

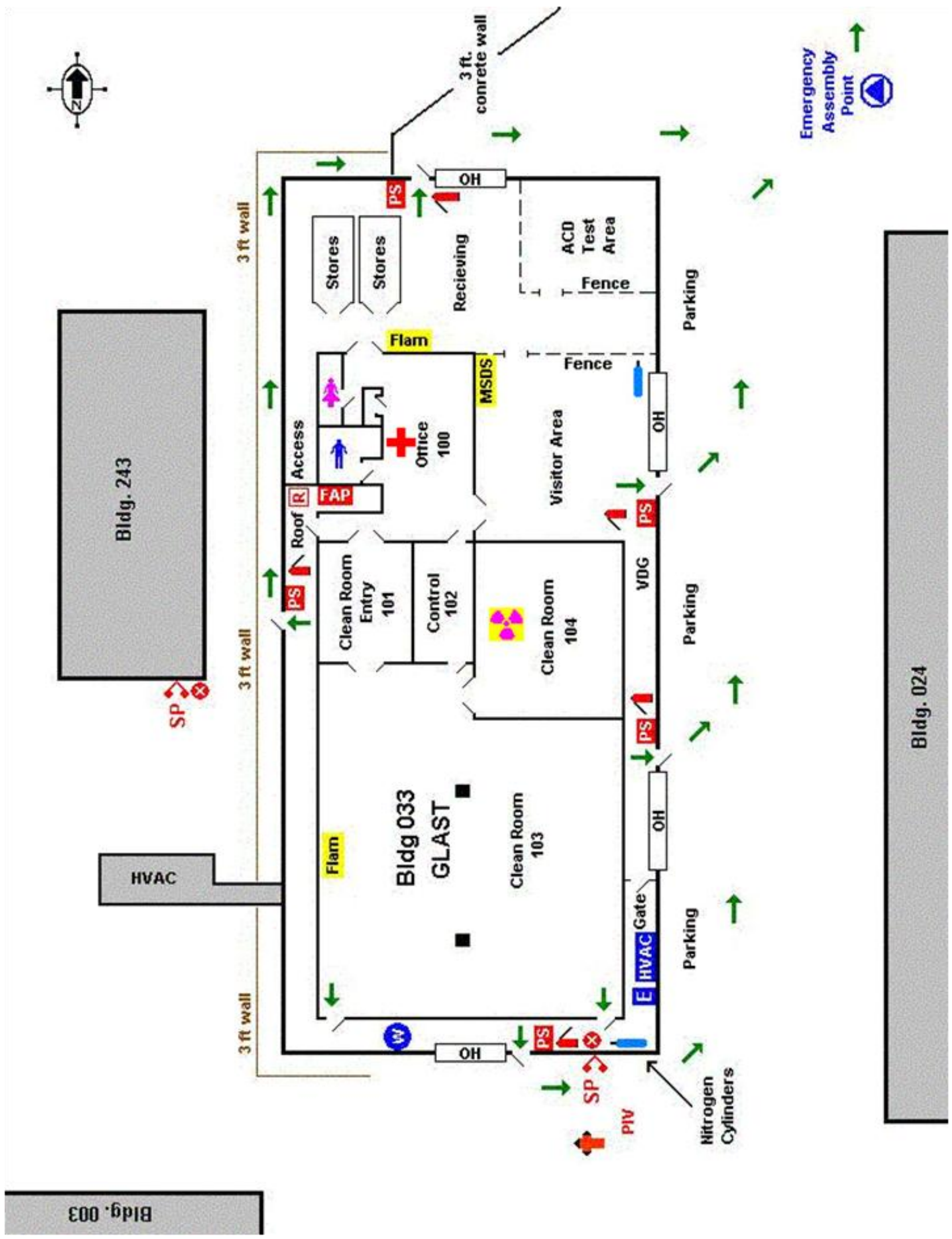
Table 5: Room volumes and maximum allowed purge gas flow rate

Room	**Dimensions and Volume**	**Maximum Purge Rate**
Room 103	75’x50’x10’ = 37,500 cu ft	200 cfh
Room 104	25’x30’x14’ = 10,500 cu ft	60 cfh
Clean tent	20’x20’x8’ = 3,200 cu ft	20 cfh

In case of complete power loss to the facility and ODM’s, we can estimate how long we can safely purge hardware as follows. For perfectly sealed rooms and a 1% drop in the oxygen percentage in no less than 8 hours, the total flow budget into each purge area is as follows: Room 103: 200 CFH, room 104: 60 CFH, Clean tent: 20 CFH.

11.4.3. Storage and Disposition of Hazardous Materials

The purchasing, use, handling, storage, transportation and disposal of all hazardous materials, as applicable to all employees, subcontractors, and users is performed in accordance to the requirements imposed in Ref [4], the SLAC ES&H Manual, Chapter 40, “Hazardous Materials.” The most common hazardous/flammable materials in use and storage are ethanol and acetone. See Figure 14 for flammable storage locations.



Water shutoff	W
Electric shutoff	E
Gas shutoff	G
HVAC shutoff	HVAC
Emergency ass'y point	
Sprinkler connection	SP
Sprinkler riser	R
PIV valve (for sprinklers)	PIV
Fire alarm Panel	FAP
Fire alarm pull station	PS
Fire extinguisher	
First aid kit	
Fire hydrant	
Roof Access	R
Exit routes	
Hazardous materials placard	
Hazardous spill kit	Spill Kit
MSDS location	MSDS
Flammable storage	Flam
Life Safety Box	LSB
Radiation Controlled area	
Compressed gas cylinders	
Roof access	R
Male/Female Restroom	

Figure 14: Layout of Building 33 emergency information

11.4.4. Crane Safety

All cranes are mechanically and electrically inspected and certified on an annual basis by SLAC. Personnel designated for crane operations need to pass course 280: SLAC OS02 "Basic Material Handling and Crane Operations Training." There are two permanent overhead traveling cranes in the facility.

Building 33, room 104, has a Top Riding Double Girder 5-ton Overhead Electric Traveling crane. The crane has a low headroom under running double girder trolley and is completely self supported with a four-post tube frame that is designed for the existing floor. The rated capacity (100 percent) is 5 tons, with maximum bridge and trolley speeds of 30 ft/min and hoist speed of 19 ft/min.

Building 33, room 101, has a Top Riding Double Girder 15-ton Overhead Electric Traveling crane. The crane has an under running double girder trolley. The crane is supported with 18 post tube frame and "I" beams designed for the existing floor. The rated capacity (100 percent) is 15 tons, with maximum speeds of 68 ft/min for the bridge, 56 ft/min for the trolley, and 13 ft/min for the hoist.

All crane lifts will be carried out using pre-defined and approved lift plans, which are part of the work planning and control plans for all operations in the facility.

11.4.5. Fire Safety

11.4.5.1. Fire Suppression Systems

The I&T facility in Building 33 includes two independent fire suppression systems. In the building high-bay, a wet-pipe sprinkler system with heat-activated heads is hung from the roof beams and covers the entire floor. This includes full coverage of the roof of the clean rooms, office spaces, and storage areas. Fire extinguishers are also located in the high-bay as well as pull-boxes.

A dry-pipe sprinkler system is installed inside the clean rooms. This covers the entire floor space of the clean rooms, and includes heat-activated heads. Fire extinguishers are also located inside the clean rooms.

11.4.5.2. Smoke Detection

A smoke detection system is also used inside the clean room. This is independent of the sprinkler system. Both the smoke detection system and oxygen deficiency monitoring systems are connected to the main facility alarm panel that automatically sends an alarm for on-site emergency response.

11.4.6. Facility Security and Access Control

Access to the I&T facilities is controlled by a nested set of access-control zones. The building and outer rooms are controlled by four levels of key-controlled access, while the clean rooms are controlled by three levels of access using Omni-lock codes. Keys and codes are assigned by the building manager or assistant building manager.

Access is restricted only to those with proper authorization and training for the facility being accessed. For the clean rooms, in particular, clean room training is currently required prior to allowing unescorted access. This training will be updated to incorporate contamination control protocols specific to the LSST Camera.