MRO Delay Line

Risk and Hazard Management

Document No. INT-406-VEN-0121

The Cambridge Delay Line Team

rev 1.0

10 Feb 2008

Cavendish Laboratory
JJ Thomson Avenue
Cambridge CB3 0HE
UK

Change Record

Revision	Date	Authors	Changes
0.1	2007-03-26	Mf	First draft version
0.2	2007-04-02	MF	Added risk tables
0.3	2008-01-10	MF	Supplemented tables
0.4	2008-02-09	MF	Tidying up and adding references.
0.5	2008-02-10	MF	Added description of risk/hazard tables
1.0	2008-02-10	MF	First released version

Objective

The objective of this document is to present the risks and hazards associated with the delivery and operation of the MROI delay line together with an assessment of the severity and the mitigations that have been assigned.

Scope

This document provides a description of the technical risks and hazards associated with providing the delay lines for the Magdalena Ridge Observatory Interferometer. It does not cover any other aspects of risk or hazards on the site or within the buildings except where there are interface issues. The identified risks and hazards are assessed individually for severity and assigned a value based on usual UK based methods. This document does not and cannot provide a complete risk assessment of the delay line installation on site. This document does not present management and schedule risks to the project.

Reference Documents

RD1 Results of the Risk Reduction Experiments (Rev 1.0 6th December 2005)

RD2 Top-level requirements INT-406-TSP-0002

RD3 Pipe Specification (Rev 8.0 25th August 2006)

RD4 Analysis of catastrophic re-pressurisation of the delay line v1.0

Applicable Documents

AD01 Pipe and Supports Drawing set

AD02 MRO Delay Line Documentation Plan INT-406-VEN-0120

AD03 Limits Design Description v0.3 INT-406-VEN-0116

AD04 Proposed Delay Line Tools, Jigs and Handling Procedures v1.0 INT-406-VEN-0119

AD05 Delay Line Pipes & Supports Design Description v1.0 INT-406-VEN-0115

Acronyms and Abbreviations

BCA Beam Combining Area

BCF Beam Combining Facility

BRS Beam Relay System

DL Delay Line

DLA Delay Line Area

ICD Interface Control Document

MROI Magdalena Ridge Observatory Interferometer

MRAO Mullard Radio Astronomy Observatory

NMT New Mexico Tech

OPD Optical Path Delay

SCS Supervisory Control System

TBC To be confirmed

TBD To be determined

Contents

Change Record 2
Objective 2
Scope 2
Reference Documents 2
Applicable Documents 2
Contents 4
1 Introduction 5
2 Risks & Hazards 5
2.1 Risk Assessment 5
2.1.1 Potential Risk - Severity: 5
2.1.2 Consequences 6
2.1.3 Probability of occurring 6
2.1.4 Risk exposure 6
2.1.5 Impact of Risk 7
2.1.6 Corrective Actions: 7
2.2 Hazard Assessment 7
2.2.1 Hazard Definitions 8
2.2.2 Hazard exposure 9
2.2.3 Hazard impact 9
3 Delay Line Risk and Hazard Management 10
3.1 Identifying the risks and/or hazards 10
4 Risk/Hazard Log 10
4.1 Risk Management – delay line pipes and supports 11
4.2 Risk Management – Trolley 12
4.3 Risk Management – Metrology System 13
4.4 Hazard Log – Delay Line Pipe 14
4.5 Hazard Log – Trolley Handling and maintenance 15
4.6 Hazard Log – Trolley Operating Conditions 16
4.7 Hazard Log – Metrology System 17

1 Introduction

The risks and hazards identified in this document have been compiled over a period of time as the project developed from the risk-reduction programme into the design and build of a prototype trolley and test rig. They have been entered into appropriate tables where the risk or hazard is defined and its potential consequences assessed and mitigated. The proposed designs that are presented for the final design review have taken into account the appropriate mitigations listed in the risk and hazard tables. Attention is drawn to the hazard to equipment and people separating it from the technical risk of equipment failure.

The assessment of the risks and hazards is based on a methodology commonly used in the UK research sector. In this document the first section briefly describes this methodology so that the method of grading the risk and hazard, together with the likelihood of an event occurring can be understood. The second section presents the risk and hazard tables which are separated into appropriate subsystems for ease of reference.

2 Risks & Hazards

Risks are generally those issues or incidences that may affect the success of the project whereas hazards affect people or equipment during the project and particularly during the service life. Risks and hazards are treated and assessed separately but in a similar way. Risk is discussed in section 2.1 together with definitions for its assessment. Hazard assessment is discussed in section 2.2 together with a similar set of definitions.

2.1 Risk Assessment

For the purposes of this document the risks here are classified as Technical Risks. They apply to the equipment designed for the delay line for the operational lifetime of the facility. The risk is assessed in two categories, the severity and the probability of occurrence. For each identified risk the product of the grading in these categories provides an overall risk exposure level which is then compared numerically to an impact rating. The evaluation of risk and impact provides a structured method for determining the course of action, if any, that should be adopted to reduce the risk exposure to an acceptable level. The definition of the two categories, the risk exposure matrix and the impact level evaluation is provided in the following subsections.

2.1.1 Potential Risk - Severity:

The severity of an event is the first major factor in an assessment and is graded regardless of the size of facility or project. Quantifications are dealt with separately in the following subsection. The severity of the risk is assigned a grade as shown in Table 1.

Table 1 Severity of Risk

Level	Designation	Definition	Implications
Low Grading 1	Minor	Minor loss of time or efficiency.	Minor effect on functionality requiring remedial action or incurring reduced efficiency/functionality.
Medium Grading 2	Moderate	Moderate $ loss, significant loss of time or efficiency	Functionality is compromised. Intervention is required or some delay is acceptable.
High Grading 3	Major Problem	Significant $ loss, severe loss of time or efficiency	Significant reduction in functionality and efficiency. Significant cost and delay.
Very High Grading 5	Catastrophe	Large $ loss	Catastrophic risk to part or all of facility. Will mean that the facility will face very significant delay.

Consequences

The consequences of a failure can be quantified according to the size of the project or facility or the subsystem that is the subject of the assessment. Possible quantifications in terms of cost and delay are given in Table 2

Table 2 Possible quantifications of consequences

Risk	Cost	Functionality	Delay
Low	Up to $50k	Slightly reduced	N/a
Medium	$50k-£100k	Moderate impact	1 month
High	$100k-£250k	Significant reduction	2 months
Very High	$250k-	Non-functional	3 months

2.1.2 Probability of occurring

The probability of an event occurring is the second major factor in the assessment. It is assigned a grading as shown in Table 3

Table 3 Probability of occurrence

Level	Designation	Definition	Grading
Low	Rare	Occur in exceptional circumstances	1
Medium	Possible	Might Occur	2
High	Likely	Quite likely to occur	3
Very High	Almost Certain	Will almost certainly occur	4

2.1.3 Risk exposure

Risk exposure is the product of the grading assigned in ‘Severity’ of the risk and the ‘Probability’ of the event occurring over the lifetime of the facility. This product can be visualised in a matrix form as shown in Table 4

Table 4 Risk exposure matrix

Probability				
Very High Grading 4	4	8	12	20
High Grading 3	3	6	9	15
Medium Grading 2	2	4	6	10
Low Grading 1	1	2	3	5
Severity	**Low** Grading 1	**Medium** Grading 2	**High** Grading 3	**Very High** Grading 5

2.1.4 Impact of Risk

Values are assigned to the severity of the risk and the probability of it occurring so that something with a high severity but a very low probability of occurrence could be assessed as requiring no mitigating action if such action was impracticable or very expensive. Conversely something that is likely to occur often but not have a severe impact (per occurrence) may score more highly, requiring mitigating action to be undertaken. The values used here are standard practise and have been used on other telescope and instrument projects.

The impact of a risk is assigned a value according to the perceived impact on the project, facility or subsystem. This value is associated with a classification of risk from low to high. Any risk classified as high must be mitigated. Any risk classified as medium should be mitigated unless mitigation is impractical or unjustifiably expensive.

Table 5 Risk impact definitions

Risk exposure	Classification	Definition
< 3	**Insignificant**	No action necessary
3-4	**Low**	Action if appropriate
5-8	**Medium**	Mitigate if possible
>8	**High**	Must mitigate

2.1.5 Corrective Actions:

Risks and risk exposure can be dealt with in the following ways:

Removal - risks are eliminated by removal of the risk situation.

Reduction – by taking certain actions or by making design changes that reduces the risk exposure.

Avoidance - risks can be anticipated and avoided by use of proper procedures.

Acceptance - the potential benefit of taking the risk outweighs the cost.

2.2 Hazard Assessment

The ALARP (As Low As Reasonably Practicable) principle will form the basis for Safety and Hazard management. A generally accepted definition of ALARP, can be summarised thus:

The principle that safety risks should be reduced to a level which is as low as reasonably practicable is the primary objective of the Safety Management System. It means that not only must risks be reduced to a tolerable level, but a further reduction must be achieved, provided that the penalties, in terms of cost, time and effort, are not disproportionate to the improvements gained.

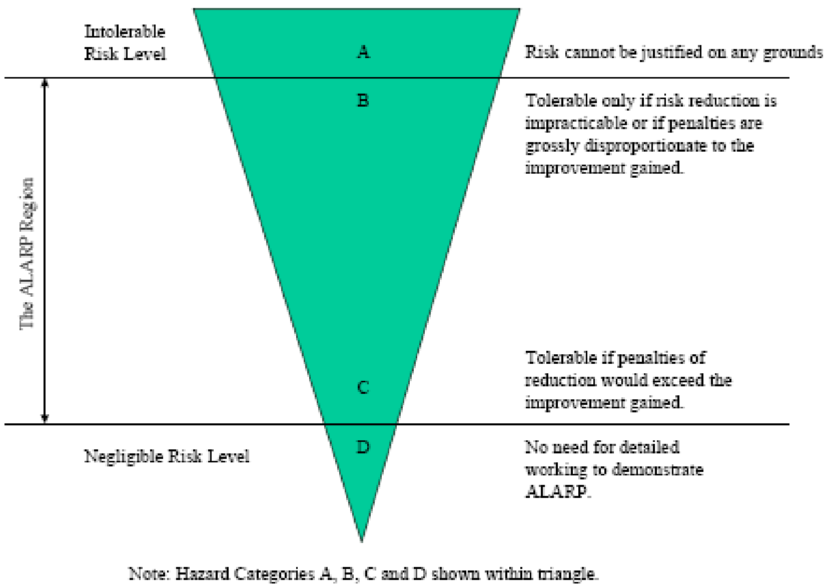

Figure 1 ALARP representation. Intolerable hazards are at the top of the triangle and negligible hazards are near the bottom. The ALARP process is to force the intolerable hazards towards the base of the triangle, bearing in mind the practicability and cost of doing so.

2.2.1 Hazard Definitions

The probability that a hazardous event is likely to occur is defined in Table 6. The timescales or the number of times an event is likely to occur is somewhat arbitrary but should be consistent with the parameters of the project. The MROI lifetime is 20 years rather than 25 years indicated in the table.

Table 6 Definition of Hazard probability

Definition	Description
Frequent A	Likely to occur frequently (≥ 6 times in 25 years)
Probable B	It will occur several times during 25 years (4-5 times in 25 years)
Occasional C	Likely to occur during 25 years (2-3 times in 25 years)
Remote D	Unlikely but possible to occur during the lifetime (typically once in 25 years)
Improbable E	So unlikely that the occurrence can be assumed not to be experienced

Table 7 Hazard severity definitions

Category	Personnel	Telescope / Systems
Catastrophic I	Death	System Loss[1]
Critical II	Severe injury[2], major occupational illness	Major system damage[3]
Marginal III	Minor injury, minor occupational illness	Minor system damage[4]
Negligible IV	Less than minor injury/occupational illness and minor system damage	

Notes:
1) *System Loss*: the system cannot be recovered at 'reasonable' costs (costs >$250k)
2) *Severe Injury*: partial permanent disability of human beings
3) *Major System Damage*; the system can be recovered (for cost of $100k - $250k) but extensive industrial support is necessary and/or the system is out of operation for more than 3 weeks.
4) *Minor System Damage*: the system can be repaired (for cost of $50k - $100k) without support from industry and/or the system is less than 3 weeks out of operation

2.2.2 Hazard exposure

Hazard exposure is the product of the grading assigned in 'Severity' of the hazard and the 'Probability' of the hazard occurring. This product can be visualised in a matrix form as shown in Table 8

Table 8 Hazard exposure matrix

	Severity Category			
Frequency of Occurrence:	Catastrophic I (=5)	Critical II (=4)	Marginal III (=3)	Negligible IV (=1)
Frequent A (=5)	25	20	15	5
Probable B (=4)	20	16	12	4
Occasional C (=3)	15	12	9	3
Remote D (=2)	10	8	6	2
Improbable E (=1)	5	4	3	1

2.2.3 Hazard impact

The impact of a hazard is assigned a value according to the perceived impact on the person or equipment. This value is associated with a classification of hazard from tolerable to unacceptable. Any risk classified as high must be mitigated. Any hazard classified as 'undesirable' should be mitigated unless mitigation is impractical or unjustifiably expensive. Any hazard classified as 'unacceptable' must be mitigated.

Table 9 hazard impact definitions

Hazard exposure	Classification	Definition
<2	**Tolerable**	ALARP Level D No action necessary
3	**Tolerable**	ALARP Level C Subject to review
4-9	**Undesirable**	ALARP Level B Only accepted if risk reduction is impracticable
10-25	**Unacceptable**	ALARP Level A Mitigating action essential

3 Delay Line Risk and Hazard Management

3.1 Identifying the risks and/or hazards

All risks and hazards should have been identified and mitigated by the FDR. Team members have reported potential hazards or risks they have identified at the weekly project meeting or by email. The team has then discussed the issues and agreed on whether risk or hazard should be entered in the risk and hazard log. If mitigation was required then a team member was allocated that task and then reported on progress in subsequent meetings.

The risk or hazard assessment was based on the following information: the location or system/subsystem; the type (risk or hazard); the target (hardware/personnel/environment);a description of the risk or hazard and the potential consequences; any potential mitigating action. Following this values were assigned:

For RISK Severity (1,2,3 or 5); Probability (1 to 4):

For HAZARD Severity (1,3, 4 or 5); Probability (1 to 5):

4 Risk/Hazard Log

The risks and hazards are tabulated separately so as to make clear the distinction between them. They are also categorised into subsystems in the following tables. These subsystems are:

(i) Delay line pipes and supports
(ii) Delay line trolley
(iii) Metrology system

A further subdivision of the trolley category is made to distinguish handling/maintenance (removal of trolley from the pipe and operating the trolley out of the pipe) and potential hazards inherent in the trolley design.

The tables present the title of the risk or hazard, the potential consequences if it occurred and the numerical assessment for the Likelihood, Effect and their product, the Score. It should be noted that the score is the result of assessment before any mitigation. The mitigation column lists the mitigations that are available. Not all possible mitigations are listed for every entry especially where they are captured by lower parts of a subsystem e.g. hardware limits will generally not accompany a mitigation which is addressed initially by range checking or software limits.

For the risk tables, attention is drawn to the high and medium risks by shading the score box. For the hazard tables, attention is drawn to the undesirable hazards by shading the score box; all the other entries are graded as ‘tolerable subject to review’. The mitigations listed are those which it is deemed reduce the risk or hazard to acceptable levels

The Risk and Hazard tables follow but first a reminder of the assigned values:

For Risks:

Severity	Score	Probability	score
Low	1	Rare	1
Medium	2	Possible	2
High	3	Likely	3
Very High	5	Almost certain	4

For Hazards:

Severity	Score	Probability	score
Negligible	1	Improbable	1
Marginal	3	Remote	2
Critical	4	Occasional	3
Catastrophic	5	Probable	4
		Frequent	5

4.1 Risk Management – delay line pipes and supports

Risk Title	Consequences	Likely-hood	Effect	Score	Mitigation
Pipes spec cannot be met	Cannot build delay line with 12 foot to 17 foot pipes.	2	3	6 medium	Use shorter pipe lengths Use different pipe technology
Pipe and supports installed in wrong position	Relative alignment of delay lines may not coincide with telescope positions. Support locations get out of step with pipe lengths.	3	2	6 medium	Accurate survey and setting of benchmarks. Accurate mark-out of support locations. Accurate control of pipe lengths
Pipe join is poor	Leads to loss of fringe tracking and therefore efficiency of observing	4	2	8 medium	Ensure pipes meet specification by inspection. RD3 Select pipes with best match Use dowelling jig to achieve accurate dowel locations in end of pipe. Check joint after assembly
Pipe seal is poor	Cannot hold vacuum for the specified period	2	2	4 low	Ensure pipe ends are clean and free from scratches immediately before assembly. Check and grease pipe seal. Carry out local pressure test after seal is fitted.
Out-gassing of seals	Not likely to compromise vacuum for long but may harm mirror coatings	2	2	4 low	Care with choice of seal material
Lifetime of seals	Seals may fail if exposed to UV light or to low temperatures	1	2	2 insig	Seals within DLA receive no UV Ensure that seals can withstand environmental specifications

4.2 Risk Management – Trolley

Risk Title	Consequences	Likely-hood	Effect	Score	Mitigation
Failure of trolley within delay line	Cannot reach trolley to restore power or correct malfunction	4	3	12 high	Incorporate recovery mechanism and procedure. DONE
Failure of trolley micro-computer or communications firmware	Trolley is stalled and unable to communicate	4	3	12 high	Implement power-on reset through inductive power system. DONE
Failure of power on board trolley	Cannot move trolley	4	3	12 high	Install on-board power storage Implement trolley rescue scheme. DONE
Breaking of inductive power/rescue cable	May not be able to rescue trolley by the designed method.	1	2	2 insig	On-board power storage of sufficient capacity if desirable.
Out-gassing of components on the trolley	Would not compromise vacuum but may affect coating on mirrors	1	3	3 low	Minimise use of materials likely to outgas. DONE
Failure of components due to vacuum.	Sealed components may rupture. Grease may be forced out of gearbox and seals.	2	2	4 low	Ensure any electronics modules are not sealed and motor/gearbox is ventilated. DONE
Failure of electronics components or modules due to lack of ventilation	Components or modules may overheat and cease to function.	3	2	6 medium	Over-rate components where possible. DONE Provide extra thermal contact to body shell. DONE
EMC	Electronics interfere with each other causing unwanted signals in sensitive circuits	3	3	6 medium	Ensure all switching modules have sufficiently different frequencies. DONE Attention to grounding on trolley chassis. Use appropriate shielding and connectors.
Sudden deceleration of trolley	Imparts significant force on to cat's eye which may damage flexures. Imparts forces to primary mirror.	4	2	8 medium	Design electronics to hold cat's eye vertical on trolley in event of 1g deceleration. DONE Incorporate 'firm' stops to limit cat's eye movement. DONE Pre-load primary mirror to withstand 3g. DONE

4.3 Risk Management – Metrology System

Risk Title	Consequences	Likely-hood	Effect	Score	Mitigation
Laser power insufficient	Can't provide for all delay lines	2	3	6 medium	Design metrology system to allow use of a second laser. DONE
Warm air from laser gets into science or metrology beams	Reduces fringe visibility	4	3	12 high	Water cool laser or channel heat away vertically into outer BCA
Warm air from shear camera gets into science or metrology beams	Reduces fringe visibility	1	3	4 low	Provide funnels to channel air above the height of the beams.
Metrology beam pointing is not sufficiently stable	Increased maintenance load. Time lost due to lost metrology lock.	2	3	6 medium	Good thermal design of metrology assembly Selection of stable metrology parts. Control of thermal environment for metrology system. Incorporate remote control of mirror adjusters. Incorporate metrology alignment aids.

4.4 Hazard Log – Delay Line Pipe

Hazard Title	**Consequences**	**Likely-hood**	**Effect**	**Score**	**Mitigation**
Re-pressurisation of delay line through catastrophic failure of science window.	Sudden air inrush causes trolley to accelerate towards far end of delay line. Potential impact at high speed causing severe damage to trolley and possible failure of pipe end-plate	1	5	5	Automatic but passive closure of window. Restricted access for personnel to area at far end of delay line during operations. Park trolley at far end of delay line. (RD4)
Re-pressurisation of delay line through catastrophic failure of Beam Relay pipe.	Sudden air inrush causes trolley to accelerate towards far end of delay line. Potential impact at high speed causing severe damage to trolley and possible failure of pipe end-plate.	2	5	10	Action by MROI Automatic closure of safety valve. (RD4)
Maximum Likely-hood Earthquake (MLE).	Weakening of pipe support system leading to pipeline collapse and potential sudden vacuum failure	2	5	10	Design supports to survive MLE. DONE Perform earthquake analysis. Perform safety analysis on design. (AD05)
Maximum Likely-hood Earthquake (MLE).	Failure of pipeline anchor leading to large axial pipe motion and potential damage to metrology system	2	4	8	Design anchor to endure MLE. DONE Perform earthquake analysis. Perform safety analysis on design. (AD05)
Accidental side-loading of a pipe line.	Due to vehicle collision. Due to handing of delay line pipe	2 3	3 3	6 9	Prevent vehicle access. Design pipe supports to withstand maximum side load under handling activities. DONE
Pipeline collapse during erection.	Damage to pipe and supports. Personal injury	3 3	4 5	12 15	Provide appropriate installation tools, procedures & training (AD04)
Pipeline collapse during maintenance.	Part of delay line may collapse when separated from the anchor section	4	4	16	Provide appropriate restraint and maintenance tools, procedures & training
Removal of inductive power anchor plug when delay line evacuated.	Loss of inductive power cable into pipe through action of cable tension and air pressure. Potential injury if fixing screws fly back.	4	3	12	Provide safety chain on anchor plug. Provide warning labels.
Over-flexing of flexural supports	Combination of maximum deflection of delay line under temperature and earthquake conditions	1	4	4	Design to accommodate maximum flexure. Take account of temperature during installation (procedure) (AD04) DONE

4.5 Hazard Log – Trolley Handling and maintenance

Hazard Title	Consequences	Likely-hood	Effect	Score	Mitigation
Dropping trolley during handling.	Dropping trolley will damage flexures and could potentially break primary mirror and deform trolley shell irretrievably.	3	3	9	Special purpose handling equipment provided together with appropriate procedures. (AD04)
Handling trolley out of delay line	Potential finger trap hazard from cat's eye and wheels when on handling trolley.	5	3	15	Provide tie down points to hold cat's eye against firm stops. Provide appropriate handling warnings on trolley.
Damage to trolley when removing from delay line	Rough handling may damage the inductive power transformer or damage cat's eye flexures	5	3	15	Provide design for handling trolley to connect to the end of the delay line. Provide handling procedures and training
Damage to trolley from frequent disassembly	Threads into aluminium may be stripped	4	3	12	Use heli-coil inserts. DONE
Accumulation of static charge on trolley.	Shock hazard when removing trolley from pipe	5	1	5	Incorporate protective measures in handling procedures. Label trolley
Operating trolley with top shell removed. Super-capacitor/battery discharge	Accidental shorting of storage power on board trolley during operation. Destruction of components and potential burn injury.	4	4	16	Enclosure of batteries or capacitors. Protection and labelling of power terminals.
Operating trolley with top shell removed.	Potential finger trap hazard from cat's eye motion	4	3	12	Provide operational maintenance procedures. Provide warning labels
Working on trolley with top shell removed – trolley powered up remotely by command	Potential trap hazard for fingers and short-circuit of supply voltages.	3	3	9	Provision of lock-off switches on utility power to inductive power system.
Working on trolley with top shell removed and trolley powered up. Unwanted commands appear through communications link.	Potential trap hazard for fingers	2	3	6	Provide operational maintenance procedures. Provide warning labels to disconnect trolley micro from wi-fi receiver

4.6 Hazard Log – Trolley Operating Conditions

Hazard Title	Consequences	Likely-hood	Effect	Score	Mitigation
Software commands trolley motion beyond end of delay line	Trolley drives into end of delay line and is damaged	3	3	9	Implement range checks where possible. DONE
Failure of communication link	Trolley cannot be stopped by command and drives into end of delay line	4	3	12	Detect link failure on board trolley and command safe state. DONE
Failure of on-board computer or software to control trolley motion	Trolley cannot be stopped or is commanded to travel at full velocity into end of delay line.	4	3	12	Implement pre-limit switches and connect to motion controller (AD03) DONE
Failure of motion controller to detect or react to limit switch	Motion controller fails or pre-limit switch interface fails.	3	3	9	Choose motion controller with in-built safety features. DONE Implement final limit to apply emergency stop to drive amplifier. IN HAND
Velocity set in excess of 1m/s	Motor cannot stop in sufficient time after a pre-limit detection	3	3	9	Minimise design motor supply voltage. Implement final limits. (AD03) IN HAND
Failure of trolley drive brushless motor amplifier	Maximum acceleration commanded	2	3	6	Minimise design motor supply voltage. Utilise amplifier with failsafe features. Install safety buffers. DONE
Failure of cat’s eye differential sensor	Leads to maximum current demand to cat’s eye voice coil and overheating of amplifier. Sudden acceleration of cat’s eye.	4	2	8	Limit circuits to protect amplifier. DONE Incorporate buffer stops on cats eye to limit and damp motion. DONE
Overheating of electronic components on board trolley	Leading to failure, thermal runaway and fumes which may affect optics	3	4	12	Over-rate components. DONE Provide thermal grounding to trolley shell. DONE

4.7 Hazard Log – Metrology System

Hazard Title	**Consequences**	**Likely-hood**	**Effect**	**Score**	**Mitigation**
Staring into metrology laser beam	Potential eye injury	4	4	16	Enclose laser beam as far as beam splitter block – after which laser beam intensity is safe. Provide standard laser hazard warnings Provide laser safety training.
Accidental reflections from metrology components	Potential eye injury	3	4	12	Provide standard laser hazard warnings Provide laser safety training.