

Delay Line Risk and Hazard Management

Martin Fisher – March 2007-03-26

Risks & Hazards

Risks are generally those issues or incidences that may affect the project whereas hazards affect people or equipment during the project and particularly during the service life. Some risks get referred to the hazard category where appropriate.

Risk Assessment

Risk can be classified as Management or Technical. There is a set of risks in each of these categories that apply to this project but it is too late and probably not worthwhile identifying all of them. Some technical risks could be identified though, specifically where the delivery of the first production trolley and the design and drawing set are concerned.

Potential Risk to project - Severity:

Level	Designation	Definition	Implications
Low Grading 1	Insignificant/Minor	No injury, low £ loss, minor loss of reputation.	Minor changes to functionality requiring remedial action or minor delay to the schedule.
Medium Grading 2	Moderate	Injuries need medical attention, significant £ loss, significant loss of reputation.	Some functionality is Compromised, requiring changes to the science specification or some delay in the schedule.
High Grading 3	Major Problem	Extensive injury, large £ loss, severe loss of reputation	Major risk of project failure to meet requirements or significant delay to schedule. Some impact on value
Very High Grading 5	Catastrophe	Potential loss of life, significant £ loss	Catastrophic risk to project. Will mean that the project will face failure or very significant delay to schedule and great overspend.

Possible quantifications

Risk	Monetary Overspend	Work Package Slip	Critical Path Slip
Low	Up to £50k	2-3 months	N/a
Medium	£50k-£100k	4-5 months	1 month
High	£100k-£250k	6-12 months	2 months
Very High	£250k+	12 months+	3 months

Probability of occurring

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

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

Impact:

Risk exposure
< 3 Insignificant
3-4 Low
5-8 Medium
>8 High

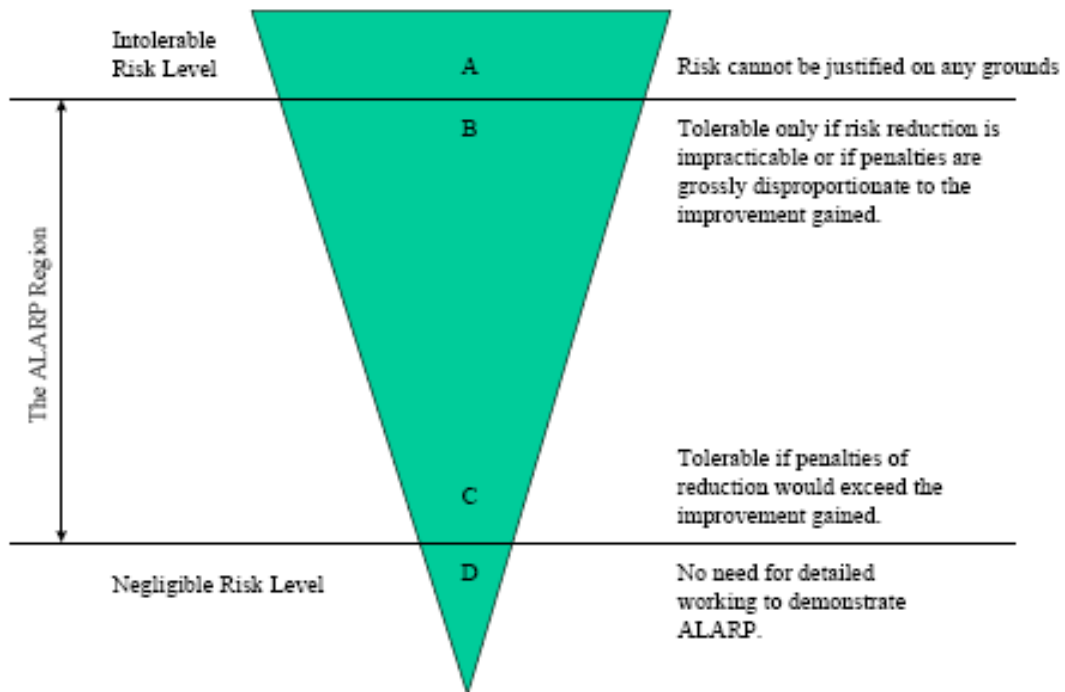
Corrective Measures:

Removal - where risks are eliminated from the project and no longer pose a threat
Reduction - by taking certain actions immediately, management can reduce risks
Avoidance - risks can be anticipated by taking contingency action should they occur.
Transfer - risks can be passed to other parties; unfortunately this does not reduce the risk it just causes someone else a problem!
Acceptance - where the potential benefits of taking the risk outweigh the costs

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.



Note: Hazard Categories A, B, C and D shown within triangle.

Definitions

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 1: Definition of Hazard Probability

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	

Table 2: Hazard Severity Definitions.

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

Frequency of Occurrence:	Severity Category			
	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

Table 3: Risk Categories expressed in Terms of Frequency and Severity.

- 1-2 Tolerable (Alarp Level D).
- 3 Tolerable subject to review (Alarp Level C).
- 4-9 Undesirable. Only accepted if risk reduction is impracticable (Alarp Level B)
- 10-25 Unacceptable. Mitigating action essential (Alarp Level A)

Risk/Hazard Log

Raising a risk or hazard issue should be done by email to the MROI team and contain the following information (note that the risk or hazard definitions and weightings should be used as appropriate)

Date raised:

Location/system/subsystem:

Who identified it:

Type (RISK/HAZARD):

Hazard target (Hardware/personnel/environment):

Description of Risk or Hazard:

Potential consequences:

Identifier's evaluation:

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

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

Mitigating Action:

The team should then discuss the issue and agree or otherwise to have it entered in the hazard log. If mitigation is required then someone should be allocated that task. The aim is to have all the hazards identified and mitigated by the FDR.

MF will keep the hazard log up to date and will input anything new to the weekly meeting at the appropriate section.

An example of the Hazard Log with some suggested items is shown on the next page.

Delay Line Risk and Hazard Management

Hazard Log

Hazard Title	Consequences	Likely-hood	Effect	Score	Mitigation
Catastrophic Re-pressurisation of delay line through window failure.	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	Automatic but passive closure of window. Restricted access to area at far end of delay line during operations.
Maximum Likely-hood Earthquake (MLE).	Weakening of pipe support system leading to pipeline collapse and potential sudden vacuum failure	2	5	10	Design pipe supports to survive MLE.
Maximum Likely-hood Earthquake (MLE).	Failure of pipeline axial restraint leading to large axial pipe motion and potential damage to metrology system	2	4	8	Design axial pipe restraint to endure MLE and limit movement of pipe.
Accidental side-loading of a pipe line.	Due to vehicle collision. Due to handing of delay line pipe	2	3	6	Prevent vehicle access. Design pipe supports to withstand maximum side load under handling activities.
		3	3	9	
Pipeline collapse during erection.	Damage to pipe and supports. Personal injury	3	4	12	Installation procedures
		3	5	15	
Accumulation of static charge on trolley.	Corona discharge Shock hazard when removing trolley from pipe	5	3	15	Prevent charge build-up Handling procedure
		5	3	15	
Dropping trolley during handling.	Dropping trolley will damage flexures and could potentially break primary mirror and deform trolley shell irretrievably.	3	4	12	Special purpose handling equipment and procedures