

# Appendix D

## Examples

This appendix provides examples of the following:

- 1 Safety policies (see chapter 3)
- 2 Hazard ranking matrix (see chapter 8)
- 3 Risk assessment (see chapter 8)
- 4 Safety Assessment remit (see chapter 14)
- 5 Safety Audit checklist (see chapter 14)
- 6 Safety Assessment checklist (see chapter 14)

## D.1 Example safety policies

This section contains extracts from the safety policies of three different rail companies:

- Railtrack plc, the infrastructure controller for the UK mainline railway,
- Virgin Trains, a UK mainline train operator,
- WS Atkins Rail Limited, a UK rail engineering and consultancy firm.

The organisations concerned have given permission for their safety policies to be included in the Yellow Book as a public demonstration of their commitment to safety. They are provided in the hope that they may prove useful to other organisations wishing to formulate safety policies. Please bear in mind that these policy statements are subject to revision. You should contact the organisations concerned directly if you wish to make sure that you have an up-to-date statement.

### D.1.1 Railtrack plc

*Railtrack plc have issued the following Safety Policy Statement.*

Railtrack PLC has prime responsibility for the safety and security of the railway it controls and for the health and safety of those who may be affected by the company's activities. As the Infrastructure Controller, our responsibility extends to ensuring safety within the entire Railway Group, through our own efforts and through the co-operation and compliance of our suppliers and the train and station operating companies that use our system. We seek and welcome recommendations for continuous improvement from both our staff and from theirs.

We view safety in the widest context - for us, it means protection from the risk of death, injury and poor health arising from our activities. It also means the avoidance of damage to property and the environment from whatever cause - accident, fire, explosion or loss of security. We will adopt a robust and cost-effective loss control policy in all that we do, recognising that good safety performance is good business - for us and our customers.

We accept that our responsibility extends to all who are involved in any way in our industry - our travellers, our workforce and those contracted to work for us, or on our property, the general public when on our property, and our neighbours.

Our commitment to a safe railway comprises:

- Improving safety through the setting of goals and targets and adherence to defined standards of excellence for all those involved in the provision of rail transport.
- The development of access and contract agreements designed to maintain a safe railway for all.
- Robust monitoring and investigation systems to enable us thoroughly to evaluate and manage risk.
- The maintenance of effective communication and systems to manage the interfaces between parties.
- A continuing policy of safety awareness for those working for our railway and all who use it.
- An intolerance of failures to establish safe methods of work or to comply with legislation, formal procedures and commitments.

Safety is fundamental to all contract and trading agreements between all parties whose activities impact on the railway. Evidence of professional safety management practice is, and will remain, a condition of access to our railway.

We will, through our operationally independent Safety and Standards Directorate, provide strategic leadership to secure the continuous improvement in safety performance necessary to deliver the ten year vision contained within the Railway Group Safety Plan.

I, as your Chairman, and the Railtrack Board, commit ourselves to uphold these principles in the efficient and effective conduct of our business and will provide adequate resources for this purpose.

Our approach to safety is dynamic and we will revise this policy to take account of any and all improvements to safety. Our policy will be reviewed at least annually.

SIR PHILIP BECK Chairman, Railtrack PLC  
August 1999

### D.1.2 Virgin Trains

*Virgin Trains issue a Health and Safety Policy as a small booklet. The policy starts with the following Chief Executive's Statement.*

#### **Nothing is more important than Safety**

Safety is the responsibility of all of us, all of the time and in everything we do. Whatever our job we each have a constant duty to ensure that there is no harm to our customers, colleagues, contractors, the general public or the environment.

Working safely is a condition of our employment and anyone who aborts work on the grounds of Health and Safety will be given my full support and that of my managers.

#### **I am committed to:-**

Continuous improvement in the Health, Safety & Welfare of all our people and all those affected by our operations, including customers, contractors and visitors.

Co-operating fully with Railtrack, other operators, and rail industry suppliers to ensure that risks to our customers, colleagues, contractors, the general public, and risks to our operations and assets, are identified and eliminated or controlled.

Setting safety performance objectives and implementing improvement actions, which will be published in our annual Safety Improvement Plan, and reviewed by Safety Council.

Ensuring adequate resources and funding are prioritised to meet our Safety commitments.

I need and acknowledge your help in eliminating hazards, which may result in personal injury, illness, fire and damage to property, harm to the environment or loss due to breaches in security.

Chris Green  
VIRGIN TRAINS June 1999

### D.1.3 WS Atkins Rail Limited

*WS Atkins Rail Limited have issued the following Safety Policy Statement.*

WS Atkins Rail is committed to implementing policies for health, safety, security and welfare and encouraging positive attitudes and behaviour. Through the WS Atkins Rail Limited Safety Policy we seek continuous improvement, compliance with legislation and standards, giving proper regard to protection of people, premises, property, processes and the environment.

All WS Atkins Rail Limited staff have a responsibility to ensure the safety of clients, colleagues, contractors and the general public. As Chairman I accept the ultimate responsibility for the safety of the organisation and I shall seek to promote a climate in which we are aware of risks and proper safeguards are taken, in line with the WS Atkins corporate Health and Safety Policy.

Suggestions from the staff on how safety arrangements can be improved and unsafe acts prevented will always be welcomed and actively encouraged within WS Atkins Rail Limited.

As head of WS Atkins Rail Limited, my Directors and I are totally committed to the implementation of these policies by personal involvement.

Safety is everyone's responsibility and a condition of our employment. We look for the support and professionalism of our employees at all levels at making this policy truly effective not only for their personal Health and Safety, but also for others whom their acts or omissions could affect.

J Doyle  
Chairman

**D.2 Example hazard ranking matrix**

The following matrix may be used in the initial ranking of hazards. The higher the rating, the more priority should be assigned to the hazard.

		Severity of Potential Harm/Loss				
		5	4	3	2	1
Safety Harm		Multiple fatalities	Single fatality	Multiple major injuries	Major injury	Minor injury
5= Daily to monthly		25	20	15	10	5
4= Monthly to yearly		20	16	12	8	4
3=1 to 10 yearly		15	12	9	6	3
2=10 to 100 years		10	8	6	4	2
1= Less than 100 yearly		5	4	3	2	1

Table D-1 - Example hazard ranking matrix

## D.3 Risk assessment

### D.3.1 Introduction

The example presented in this appendix is provided to illustrate application of the risk assessment framework detailed in this document. The example does not necessarily relate to actual operational circumstances and **the data used within the example is provided for the purposes of illustration only**. In order to simplify the example, some crude assumptions have been made that are unlikely to apply in practice.

### D.3.2 Background to example

The undertaking subject to analysis is the operation of an Automatic Half Barrier level crossing in a particular location. There is scope for making improvements to the operation and use of this system. The aim of this risk assessment is therefore to determine whether changes are required in order to reduce the risk presented by the particular Automatic Half Barrier to a level that is compliant with the principle of ALARP.

It should be noted that the Automatic Half Barrier concerned has, to date, been in operation for a period of 20 years. There is, therefore, some considerable operational experience of its use.

### D.3.3 Hazard Identification

The operation of an Automatic Half Barrier level crossing is not a novel process. Hence the hazards associated with this undertaking were predominantly identified from a checklist.

The likely frequency and severity of each hazard has been estimated using the categorisation detailed in Table D-2 and Table D-3.

For each hazard, its estimated frequency and severity have been multiplied to obtain the hazard's 'rank'. Table D-4 presents the results of hazard identification and ranking.

<b>Frequency category</b>	<b>Definition</b>
1	Less than 100 yearly
2	10 to 100 years
3	1 to 10 yearly
4	Monthly to yearly
5	Daily to monthly

**Table D-2 - Categorisation for estimated hazard frequency**

<b>Severity category</b>	<b>Definition</b>
1	Minor injury
2	Major injury
3	Multiple major injuries
4	Single fatality
5	Multiple fatalities

**Table D-3 - Categorisation for estimated hazard severity**

Hazard Ref.	Hazard Description	Estimated Frequency	Estimated Severity	Hazard Rank	Comments/Rationale
1	Works Crossing is Used When Not Authorised	N/A	N/A	N/A	The crossing under analysis is not a works crossing. Hence, this hazard is not relevant
2	Failure of Level Crossing to Protect Public From Train	2	4	8	During the period for which this crossing has been in operation (20 years), no such failure has occurred. The low traffic supported by this crossing reduces the hazard severity
3	Barrier Operates Without Being Caused By Train	3	4	12	Failures of this type result mainly in service disruption. However, there is a possibility that subsequent manual operation of the barrier will result in an accident
4	Misuse of Level Crossing by Road User	4	2	8	Accidents of this type are most likely to result from a road user swerving around the closing barriers. The most likely consequence is impact with the infrastructure, resulting in a major injury
5	Use of Crossing Exceeds Original Design Limits	N/A	N/A	N/A	The current use of the crossing is well within the original design limits
6	SPAD at Signal Protecting Level Crossing	1	4	4	During the period for which this crossing has been in operation, no such SPAD has occurred. Additionally, the long signal overlap would mitigate most occurrences of this hazard
7	Poor Sighting of Level Crossing	5	4	20	Risks associated with poor sighting of the crossing occur each time a road user approaches the crossing when it is in use by a train.

Table D-4 - Results of hazard identification

### D.3.4 Causal Analysis

Causal Analysis has been conducted to estimate the annual frequency of occurrence of each of the hazards. The depth of the analysis undertaken has varied according to the relative rank of each hazard.

For the purposes of this illustrative example, only the results of Causal Analysis of Hazard 2 are presented – 'Failure of Level Crossing to Protect Public from Train'. The simple fault tree constructed to evaluate the frequency of occurrence of the hazard is presented in Figure D-1.

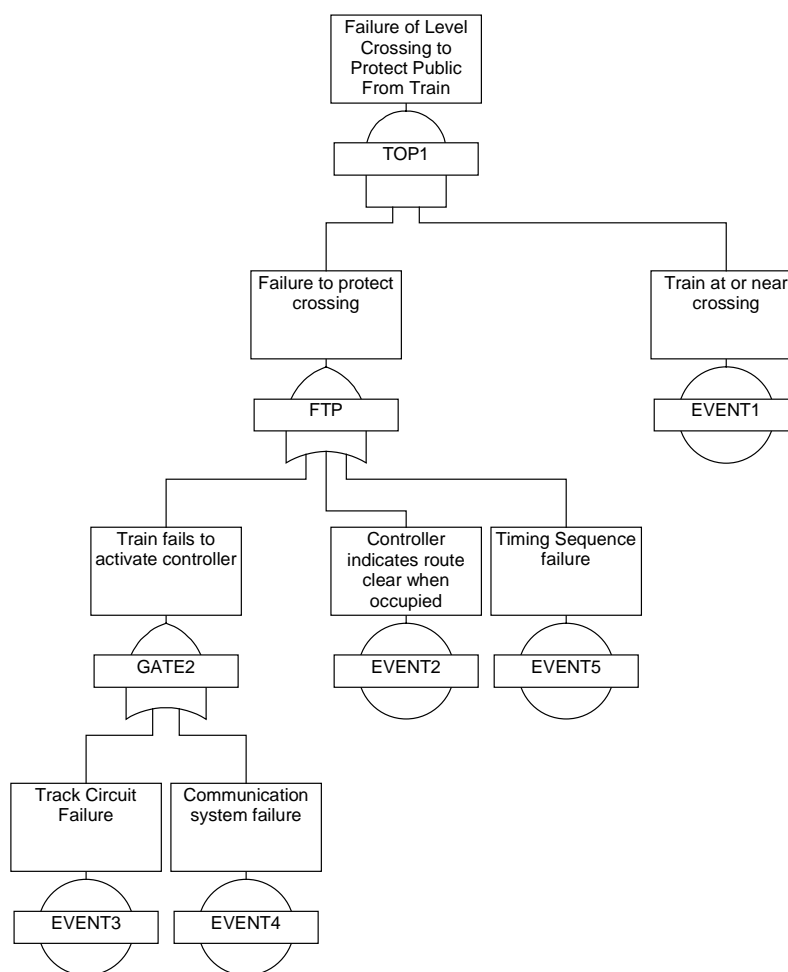


Figure D-1 - Fault tree for hazard 2

The fault tree has been quantified on the basis of the following analysis:

- From examination of the timetable it has been determined that an average of four trains traverse the crossing per hour. Protection is required for the crossing of each train for a period of approximately 90 seconds. At any time, therefore, the probability of the event 'Train at or near level crossing' is as follows:

$$\text{Probability} = \frac{90 \times 4}{3600} = 0.1$$

- There is some considerable operational experience of use of the level crossing controller employed at this crossing, both within the Railtrack network and overseas. On the basis of the records of this experience, it has been determined that the probability of the event 'Controller indicates route clear when occupied' is  $5.0 \times 10^{-3}$  per annum per controller.
- Similarly, there is considerable experience of use of the particular type of track circuit employed in this undertaking to indicate the presence of an approaching train to the level crossing controller. Records maintained by Railtrack suggest that, for the rolling stock type used on the line concerned, the probability of the event 'Track circuit failure' is  $2.5 \times 10^{-3}$  per annum.
- An independent contractor has previously been employed by Railtrack to determine the likelihood of failure of communications to the level crossing controller. Analysis conducted by this contractor suggests that the probability of the event 'Communication System Failure' is  $1.5 \times 10^{-3}$  per annum.
- The event 'Timing Sequence Failure' covers the situation when there is a pedestrian or vehicle on the crossing when the barriers fall. Operational experience gained from use of the level crossing suggests that slow moving pedestrians and traffic cause protection to be removed from this crossing twice per year on average. Hence the probability of the event 'Timing Sequence Failure' is 2.0 per annum.

Using the above values of each of the fault tree base events, the probability of Hazard 2 has been determined as follows:

$$\text{Probability} \approx \left( (2.5 \times 10^{-3} + 1.5 \times 10^{-3}) + 5.0 \times 10^{-3} + 2.0 \right) \times 0.1 = 0.20$$

Note that the probability of the hazard is dominated by the probability of the event 'Timing Sequence Failure'.

### D.3.5 Consequence Analysis

Consequence Analysis has been conducted to determine those incidents, which may arise from occurrence of each of the hazards. The depth of the analysis undertaken has varied according to the relative rank of each hazard, in a similar manner to that for Causal Analysis.

For the purposes of this illustrative example, only the results of Consequence Analysis of Hazard 2 are presented – 'Failure of Level Crossing to Protect Public from Train'. The particular method of consequence analysis used to analyse this hazard is the 'Cause Consequence' modelling technique. This is an inductive method of analysis where the hazard under consideration is displayed at the bottom of a decision-tree structure. Possible protective barriers affecting event escalation are then identified, classified and assessed. The potential outcomes (consequences) as a result of success or failure of the barriers are presented at the top of the page. The consequences can range from benign, essentially safe conditions to major or catastrophic accidents.

The simple cause-consequence models constructed to investigate the consequences of Hazard 2 are presented in Figure D-2. The consequences to pedestrians and other road users are modelled separately.

For the purposes of this analysis it has been estimated that, on average, 500 pedestrians use the crossing per day, taking 9 seconds each to traverse the crossing. Since trains run for 15 hours per day on this line, this leads to the following probability of a pedestrian being present at the crossing at any given time whilst trains are running:

$$\text{Probability} = \frac{500 \times 9}{3600 \times 15} = 8.3 \times 10^{-2}$$

Similarly, to estimate the probability of a road user being present at the crossing it has been estimated that, on average, 1000 vehicles use the crossing per day, taking 5 seconds to traverse the crossing.

It can be seen from the analysis, that most occurrences of the hazard do not lead to an accident, due to mitigating factors such as the vigilance of pedestrians and other road users and other, circumstantial factors, such as there being no traffic at the crossing when the hazard occurs.

*Note: The estimates of the probability with which a vehicle or pedestrian takes successful emergency action have to take account of the fact that, in most cases where the hazard occurs, it is as a result of a slow moving vehicle or pedestrian in the first place.*

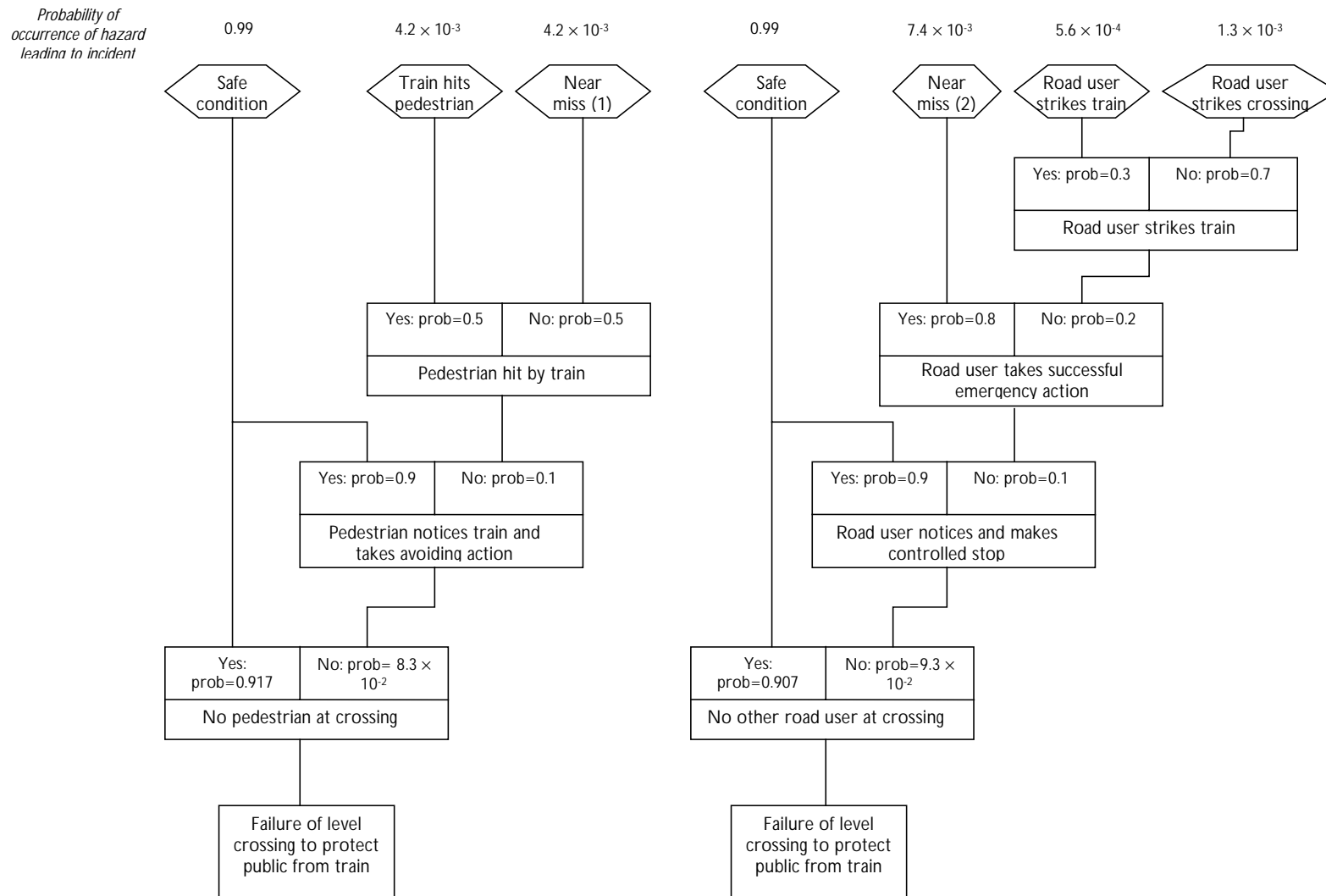


Figure D-2 - Cause-consequence models for Hazard 2

### D.3.6 Loss Analysis

Loss Analysis has been conducted to determine the magnitude of potential safety losses associated with each hazard.

For the purposes of this illustrative example, only the results of Loss Analysis of Hazard 2 are provided – 'Failure of Level Crossing to Protect Public from Train'. Table D-5 presents details of the loss modelling conducted. The incidents (consequences) have been taken from the cause consequence diagram presented earlier. The following incidents were identified:

- Safe Condition,
- Near Miss,
- Train Hits Pedestrian,
- Road User Strikes Train,
- Road User Strikes Crossing.

It has been assumed that no losses arise from a Safe Condition. A Near Miss is judged not to result in safety losses, although it can result in significant train delays. The remaining consequences all result in both safety and commercial losses.

Following analysis of Railtrack accident statistics, for circumstances similar to the level crossing under study, it has been assumed that:

- the incident 'Train Hits Pedestrian' results in no injuries to passengers, but 1 fatality to a member of the public;
- the incident 'Road User Strikes Train' results in 2 minor injuries to passengers and a single major injury to a member of the public;
- the incident 'Road User Strikes Crossing' results in 1 minor injury to passengers and 1 major injury to a member of the public.

The injuries associated with each incident have been converted to a corresponding Potential Equivalent Fatality (PEF) figure using the following currently accepted Railtrack convention:

- 1 fatality = 10 major injuries
- 1 major injury = 20 minor injuries

Incident	Frequency (per annum)	Safety loss per incident (PEF)		Safety loss per annum (PEF)	
		Passenger	Public	Passenger	Public
Train Hits Pedestrian	$8.4 \times 10^{-4}$	-	1	-	$8.4 \times 10^{-4}$
Near Miss (1)	$8.4 \times 10^{-4}$	-	-	-	-
Near Miss (2)	$1.5 \times 10^{-3}$	-	-	-	-
Road User Strikes Train	$1.1 \times 10^{-4}$	$10^{-2}$	0.1	$1.1 \times 10^{-6}$	$1.1 \times 10^{-5}$
Road User Strikes Crossing	$2.6 \times 10^{-4}$	$5 \times 10^{-3}$	0.1	$1.3 \times 10^{-6}$	$2.6 \times 10^{-5}$
Total per annum				$2.4 \times 10^{-6}$	$8.8 \times 10^{-4}$

**Table D-5 - Results of Loss Analysis for hazard 2**

It should be noted that, in order to demonstrate compliance with the ALARP criteria, in a subsequent stage of risk assessment, safety losses have been determined individually for the following Groups defined by Railtrack as exposed to the risk of railway operations: passengers and the public. The hazard has not been determined to lead to any losses to employees (trackside workers).

The annual frequency of each incident has been determined by multiplying the estimated frequency of the hazard (derived during Causal Analysis) by the estimated probability of the hazard leading to the incident once the hazard has occurred (derived during Consequence Analysis).

Commercial losses have been estimated by means of expert judgement and through knowledge of previous incidents.

### D.3.7 Options Analysis

Both structured brainstorming and a suitable checklist have been used to identify potential risk mitigation options for each hazard. The checklist that has been used records known mitigation measures employed elsewhere throughout the Railtrack network. Use of brainstorming and the checklist together provide a high degree of confidence that all significant options for risk mitigation have been identified.

Table D-6 summarises those risk mitigation options that have been identified.

Option costs have been derived from knowledge of previous application of protective measures at similar level crossings and, for measures such as provision of Automatic Train Protection, through use of expert judgement.

### D.3.8 Impact Analysis

Each of the potential risk mitigation options identified in the previous stage of risk assessment have been analysed further to determine their effects upon the losses associated with operation and use of the level crossing.

Estimates of the reductions in losses achieved through use of each option have been calculated by modifying the Causal or Consequence models associated with the option (developed in the previous stages of risk assessment).

Hazard Ref.	Hazard Description	Hazard Rank	Option	Option Cost (£ pa)
2	Failure of Level Crossing to Protect the Public From Passing trains (Wrong Side Failure of Level Crossing)	8	1. Modify crossing to have more reliable controller	750
			2. Modify crossing sequence to provide greater crossing time	750
			3. Rewire cables to controller to replace degraded cabling	1000
4	Barrier Operates Without Being Caused By Train	12	4. Provide CCTV to protect crossing from vandalism/abuse	2500
5	Misuse of Level Crossing by Road User	8	5. Provide warning signs at approach to level crossing	300
7	SPAD at Signal Protecting Level Crossing	4	6. Provide Automatic Train Protection	20000
8	Poor Sighting of Level Crossing	20	7. Provide warning signs to indicate to road user the state of route ahead	2000
			8. Re-routing of approaching road	50000

**Table D-6 - Results of Options Analysis**

For the purposes of this illustrative example, only the results of the analysis of one of the options are presented – modify crossing sequence to provide greater crossing time. To further analyse this option it has been estimated that by increasing the crossing time, the probability of the event 'Timing Sequence Failure' can be reduced by an order of magnitude.

Applying this revised failure probability within the previous causal analysis of the hazard leads to a reduced annual probability of occurrence of the hazard of  $2.1 \times 10^{-2}$ . The loss analysis conducted previously has therefore been revised and the results of this revised analysis are presented in Table D-7.

Incident	Frequency (per annum)	Safety loss per incident (PEF)		Safety loss per annum (PEF)	
		Passenger	Public	Passenger	Public
Train Hits Pedestrian	$8.8 \times 10^{-5}$	-	1	-	$8.8 \times 10^{-5}$
Near Miss (1)	$8.8 \times 10^{-5}$	-	-	-	-
Near Miss (2)	$1.6 \times 10^{-4}$	-	-	-	-
Road User Strikes Train	$1.2 \times 10^{-5}$	$10^{-2}$	0.1	$1.2 \times 10^{-7}$	$1.2 \times 10^{-6}$
Road User Strikes Crossing	$2.7 \times 10^{-5}$	$5 \times 10^{-3}$	0.1	$1.4 \times 10^{-7}$	$2.7 \times 10^{-6}$
Total losses per annum (with mitigation) – (A)				$2.6 \times 10^{-7}$	$9.2 \times 10^{-5}$
Total losses per annum (without mitigation) – (B)				$2.4 \times 10^{-6}$	$8.8 \times 10^{-4}$
Total mitigated losses per annum (B-A)				$2.1 \times 10^{-6}$	$7.9 \times 10^{-4}$

**Table D-7 - Revised Loss Analysis assuming modified crossing sequence time**

### D.3.9 Demonstration of ALARP and Compliance

Railtrack currently define three Groups exposed to the risks of their operations: employees (trackside staff), passengers and the public.

Table D-8 details the ALARP and Benchmark criteria currently adopted by Railtrack for each Group and specified in Railtrack's Railway Safety Case. Each of the values represents an average risk of fatality per annum for an individual in the respective Group.

Group	Upper Limit of Tolerability	Broadly Acceptable bound	Benchmark
Employee	$10^{-3}$	$10^{-6}$	$10^{-4}$
Passenger	$10^{-4}$	$10^{-6}$	$10^{-5}$
Public	$10^{-4}$	$10^{-6}$	$10^{-5}$ §

**Table D-8 - ALARP and Benchmark criteria currently employed by Railtrack for all of its operations**

§ It should be noted that Railtrack's actual Benchmark figure is lower than this value. This value is however used for the purposes of this illustrative example

Previous investigations and analysis conducted by Railtrack suggest that automatic half barrier level crossings contribute 10%, 20% and 50% of the total risk of all of Railtrack's operations, to Employees, Passengers and the Public respectively.

There are known to be 300 such crossings in the Railtrack network. Whilst some crossings are known to pose slightly increased risk compared to others, analysis conducted by Railtrack suggests that the majority of crossings are associated with similar risk levels.

Hence, it can be assumed that the fraction of Railtrack's total safety risk which is associated with a single automatic half barrier level crossing is as follows:

$$\begin{aligned} \text{Fraction of total safety risk to Employees} \\ \text{associated with a single crossing} \end{aligned} = (1 \times 0.1) / 300 = 3.3 \times 10^{-4}$$

$$\begin{aligned} \text{Fraction of total safety risk to Passengers} \\ \text{associated with a single crossing} \end{aligned} = (1 \times 0.2) / 300 = 6.7 \times 10^{-4}$$

$$\begin{aligned} \text{Fraction of total safety risk to Public} \\ \text{associated with a single crossing} \end{aligned} = (1 \times 0.5) / 300 = 1.7 \times 10^{-3}$$

The apportioned ALARP and Benchmark criteria which the level crossing under consideration should meet can therefore be determined by multiplying the criteria given in Table D-8 by the above fractions. The resulting apportioned criteria are given in Table D-9.

Group	Apportioned Upper Limit of Tolerability	Apportioned Broadly Acceptable bound	Apportioned Benchmark
Employee	$3.3 \times 10^{-7}$	$3.3 \times 10^{-10}$	$3.3 \times 10^{-8}$
Passenger	$6.7 \times 10^{-8}$	$6.7 \times 10^{-10}$	$6.7 \times 10^{-9}$
Public	$1.7 \times 10^{-7}$	$1.7 \times 10^{-9}$	$1.7 \times 10^{-8}$

**Table D-9 - Apportioned ALARP and Benchmark criteria for the undertaking concerned**

In order to determine the total safety losses associated with the undertaking, the estimated safety losses associated with each of the hazards, prior to application of mitigation measures, have been summed together. The results of this summation are presented in Table D-10 (note that only the estimated safety losses associated with Hazard 2 have previously been presented as part of this illustrative example).

Group	Total Safety Losses Associated with Undertaking per annum
Employee	0
Passenger	$5.2 \times 10^{-7}$
Public	$8.0 \times 10^{-4}$

**Table D-10 - Total safety losses associated with undertaking per annum**

It is estimated that, on average, 10000 different individuals are regular daily users of the crossing. The average risk to each of these individuals, associated with the undertaking, is therefore as presented in Table D-11. It should be noted that significantly more than 10000 different individuals use the crossing per year. However, outside of the 10000 regular daily users, other individuals use the crossing very infrequently and are not therefore considered in this risk apportionment.

Group	Average Safety Losses per Individual per annum
Employee	0
Passenger	$5.2 \times 10^{-11}$
Public	$8.0 \times 10^{-8}$

**Table D-11 - Average safety losses per individual associated with undertaking per annum**

Comparison of the average individual risk with the apportioned ALARP and Benchmark criteria suggests that the risks to employees and passengers fall below the Apportioned Broadly Acceptable Bound. However, the average risk to a member of the public falls within the tolerability region (above the Apportioned Broadly Acceptable Bound and below the Apportioned Upper Limit of Tolerability). It is therefore necessary to determine those risk mitigation measures which should be applied in order to reduce risks to ALARP levels.

For the purposes of this exercise we use a VPF of £1.63M.

Table D-12 presents a summary of each of the risk mitigation options and the annual reductions in safety losses to which they may lead (note that only the reductions in safety losses associated with modified crossing sequence time have previously been presented as part of this illustrative example). The table employs the VPF value detailed above. Net costs are derived by subtracting any mitigated commercial losses from the direct costs.

Risk mitigation option	Direct costs per annum (£)	Net costs per annum (£)	Annual mitigated safety loss (PEF)	Annual monetary value of mitigated loss (£)
1	750	710	$3.9 \times 10^{-5}$	64
2	750	690	$7.9 \times 10^{-4}$	1300
3	1000	950	$9.1 \times 10^{-5}$	150
4	2500	2400	$6.3 \times 10^{-5}$	100
5	300	290	$2.3 \times 10^{-5}$	37
6	20000	20000	$7.1 \times 10^{-5}$	120
7	200	1900	$5.6 \times 10^{-5}$	91
8	50000	49000	$6.3 \times 10^{-5}$	100

**Table D-12 - Cost-benefit analysis of potential risk mitigation options**

It can be seen that only option 2 is reasonably practicable to implement. Hence, the risks associated with the undertaking are reduced to ALARP levels through implementation of option 2 only and without any further mitigation measures.

The residual risk of the undertaking after implementation of option 2 is as follows:

$$\text{Residual risk} = 8.0 \times 10^{-4} - 7.9 \times 10^{-4} = 1.0 \times 10^{-5} \text{ per annum}$$

The average residual risk to the 10000 regular daily users of the crossing is therefore  $1.0 \times 10^{-9}$  per annum. This is less than the apportioned Railtrack benchmark.

## D.4 Safety Assessment remit

The following generic wording is used and recommended by the Railtrack System Review Panels as a starting point for writing remits for safety assessments:

*The assessment shall:*

- *State the safety targets which have been used in carrying out the assessment.*
- *Give a professional recommendation on the suitability and acceptability of the document with regard to its stated purpose.*

*The critical and most sensitive arguments of the documents should be clearly and concisely highlighted and a professional opinion shall be given as to the robustness of the argument. Where the argument of contained in whole or part within other documents or is part of existing custom and practice this should be clearly identified.*

*A professional opinion should also be given, with regard to the railway system as a whole, as to the practicality of any measures used to mitigate against the hazards raised.*

- *Identify any non-compliances to Railway Group or Railtrack Line Standards and legal requirements.*
- *Supply related technical advice as required by the Client, or as perceived necessary by the advisor.*

*All assessor observations are to be uniquely numbered and classified into one of the following three Classes, categories 1 to 3 should be used where operational use is being sought and categories A to C where other documents are under review (additional subclasses are permitted to aid clarity):*

### ***Documents seeking Operational Authority***

*Category 1 Issue is sufficiently important to require (substantial) resolution, prior to recommending that the train/equipment may become operational. (Alternatively a specific control measure may be implemented to control the risk in the short term).*

*Category 2 Issue is sufficiently important to require resolution within 3-6 months, but the train/equipment may become operational in the interim (possibly with a protective control measure).*

*Category 3 Issue is highlighted for incorporation into the Safety Case at the next periodic review, but no action is required separately.*

***Other Documents***

*Category A* Concerns, errors, omissions or questions that have a direct bearing on the acceptability of the document, which it is necessary to resolve prior to the consideration of downstream or offspring documents.

*Category B* Requires satisfactory resolution prior to acceptance of complete safety submission, or within a defined time period (not normally to exceed 6 months).

*Category C* Minor errors, e.g. syntax, spelling, minor technical matters which have no direct significant safety implications. For clarity, these require to be recorded and correcting if the document is re-issued, but are not in themselves sufficiently significant to warrant re-issue on their own.

*For either the numerical or alphabetical categories, where there are a large number of lower category issues, the reviewer is to consider whether in totality they represent sufficient residual risk that they in effect equate to one or more higher category issues (e.g. that they would warrant the imposition of any additional mitigating control measures). In these circumstances, It should be considered whether these outstanding issues relate to an overall lack of rigour or quality in the document which has been reviewed.*

## D.5 Safety Audit checklist

### D.5.1 Pro forma

This section presents a pro forma for each question in the audit checklist. Each question should be entered and given a unique reference. Following the audit the answer should be ringed, evidence to support the answer entered and the impact of the answer indicated. Conformance should be indicated by ringing *OK*; or category *A*, *B* or *C* (see chapter 14). Any further comments should also be noted.

Question: <Enter question>	Ref: <Enter unique reference>
Evidence: <Enter supporting evidence>	Yes    No    n/a <Ring answer>
Comments: <Enter any other comments, if any>	OK    A    B    C <Ring impact>

### D.5.2 Example audit checklist

This section contains typical questions that might be asked during a Safety Audit. It is intended to be an example and is neither exhaustive nor mandatory.

Where a question asks if something is adequate, judgement from the Safety Auditor is required, taking into account explanations provided by the Project Manager. In general something is adequate if:

- it meets specified requirements;
- it is effective and economical;
- it is appropriate to the circumstances; and
- it represents best practice.

#### D.5.2.1 Safety planning

- a) Is there an adequate Safety Plan (see chapter 12)?
- b) Are the responsibilities for safety and the competencies of staff clearly defined?
- c) Is the Safety Plan clear, easily obtained and accessible to the project?
- d) Have appropriate safety requirements been defined for each deliverable?
- e) Have suitable controls been devised to verify the safety requirements?
- f) Has an appropriate approach to safety been chosen?

#### D.5.2.2 Safety documentation

- a) Has the Safety Documentation required for the project been identified?
- b) Has the identified documentation been produced?
- c) Is the plan for safety documentation adequate?
- d) Have the responsibilities for producing safety documentation been identified?
- e) Has the documentation been produced by the staff identified for the task?
- f) Has an appropriate standard for documentation been specified?
- g) Has the standard been consistently applied?

#### D.5.2.3 Subcontract management

- a) Has an adequate method of evaluating subcontractor capability been identified?
- b) Has this method been rigorously applied to all subcontractors?
- c) Has each subcontractor been set safety targets or requirements?
- d) Has each subcontractor produced a Safety Plan?
- e) Have these plans been reviewed and approved as defined in the project Safety Plan?
- f) Is there any evidence of subcontractor non-compliance?
- g) Have all subcontractor-identified hazards been entered in the Hazard Log?

#### D.5.2.4 Testing

- a) Has testing called for in the Safety Plan been carried out?
- b) Is the test team independent of the development team?
- c) Have incidents arising from testing activities been entered in the Hazard Log?
- d) Does the testing programme adequately demonstrate the safety of the system?

## D.6 Safety Assessment checklist

Where a checklist question relates to a document or a task, the current section providing guidance for that document or task should be consulted. These have not been identified in the checklists to avoid extensive updating when changes are introduced.

Questions marked with an asterisk may require comments to be recorded separately and referenced accordingly.

### D.6.1 Commissioning an assessment

Checklist for person writing requirements:

- a) Safety Assessor has sufficient independence (see chapter 14);
- b) Safety Assessor has sufficient qualifications and experience (see chapter 14);
- c) Requirements have been discussed with Project Manager;
- d) Remit has been signed by originator;
- e) Remit has been signed by Safety Assessor;
- f) Remit has been copied to Safety Assessor and Project Manager.

### D.6.2 The assessment process

Checklist for Safety Assessor:

- a) For the system to be assessed, has the following documentation been checked:
  - Safety Plan?
  - Hazard Log?
  - Safety Requirements Specification?
  - Specification?
  - Drawings?
- b) Have safety requirements been identified in the documentation listed above?
- c) Having read the above documentation do you have any questions or points of doubt over the requirements? \*
- d) Has the system been identified functionally by means of block diagrams?
- e) Do the block diagrams cover levels of the systems from the highest down to line replaceable units?
- f) Do the block diagrams adequately represent the system as specified?
- g) Is there design documentation showing reasons for decisions made in the system design process?
- h) Do you have any comments or recommendations regarding the design disclosure document? \*
- i) Has a hazard list been compiled?
- j) Have hazards been removed/mitigated where appropriate?

- k) Do you have any comments or recommendations concerning the hazard list? \*
- l) Has a list of potential accidents been compiled?
- m) Do you have any comments or recommendations on the list of potential accidents? \*
- n) Have any novel or unproved features in the design been noted so that particular attention can be given to resolving any safety problems?
- o) Do you have any comments or recommendations regarding the novel or unproved features? \*
- p) Has any information been compiled on the safety of similar systems?
- q) Do you have any comments or recommendations on the information provided on similar systems? \*
- r) Have accident sequences been analysed for each type of potential accident?
- s) Do you have any comments on the accident sequence analyses? \*
- t) Have risk assessments been made?
- u) Has the risk been reduced ALARP?
- v) Have risk classifications been made?
- w) Have tolerable risk levels been agreed?
- x) Have accident rate targets been set?
- y) Have hazard rate targets been set?
- z) Have Safety Integrity Levels been determined for the safety elements of the design?
- aa) Has the design been assessed against the targets for the random elements of the design?
- ab) Has the design been audited against the design rules implied by the Safety Integrity Level?

### D.6.3 Assessment checklist: Requirements definition

Checklist for Safety Assessor:

- a) For the system to be assessed, have the following documents been checked:
  - Feasibility Studies Reports?
  - Statement of Requirements?
  - Drawings?
- b) Have safety targets or requirements been given in the following documents:
  - Feasibility Studies Reports?
  - Statement of Requirements?

- c) Having read the above documents, do you have any questions or areas of doubt in the requirements? \*
- d) Has a Safety Plan been prepared?
- e) Do you have any comments or recommendations concerning the Safety Plan? \*
- f) Has a Hazard Log been started?
- g) Do you have any comments or recommendations regarding the Hazard Log? \*
- h) Has the system been identified, in schematic or functional drawings?
- i) Has failure mode effect analysis been done?
- j) Do you have any comments or recommendations concerning the failure mode effect analysis? \*
- k) Have accident sequences been considered?
- l) Do you have any comments on potential accident sequences, hazards, initiating events or contributory incidents? \*
- m) Have the severities or consequences of potential accidents been determined or classified?
- n) Do you have any comments on accident severity or consequence classification? \*
- o) Has the design been altered during project definition to reduce hazards?
- p) Do you have any comments or recommendations concerning hazard reduction? \*
- q) Have the probabilities or frequencies of initiating events been determined?
- r) Do you have any comments or recommendations on the likelihood of initiating events or hazards? \*
- s) Has a Risk Assessment criteria for determining tolerability been drawn up?
- t) Does target apportionment take into account the expected number of units in service?
- u) Do you have any comments on the determination of the tolerability of risk? \*
- v) Have risks been determined for all aspects of the design? \*
- w) Are there aspects of the design which you would recommend for further risk assessment? \*
- x) Does the specification for design and development contain safety targets and requirements?
- y) Do you have any comments on the specified targets or requirements? \*
- z) Have safety targets been allocated to the lower level functions?
- aa) Do you have any comments or recommendations on the allocation of safety targets? \*

#### D.6.4 Assessment checklist: Design, build and test

Checklist for Safety Assessor for use during system design, implementation, and testing:

- a) Has a Safety Plan been formally issued?
- b) Do you have any comments or recommendations concerning the Safety Plan? \*
- c) Has a Hazard Log been started and maintained?
- d) Do you have any comments or recommendations on the contents of the Hazard Log? \*
- e) Is the system design well-defined?
- f) Have the safety-related parts of the system been made as simple as possible?
- g) Have safety-related sub-systems been identified?
- h) Has there been any development of the design to remove undesirable features or improve performance characteristics?
- i) Are there any potential accidents associated with the design? \*
- j) Have the potential accident sequences been adequately examined? \*
- k) Have Design Reviews been carried-out?
- l) Do you have any comments or recommendations on the Hazard Identification and Analysis work?
- m) Has Risk Assessment been carried out?
- n) Does this table take into account the expected number of units in service?
- o) Do you have any comments or recommendations concerning the assessment of risks? \*
- p) Have tolerable levels of risk been established?
- q) Is the tolerability of risk consistent with the relevant industry standards?
- r) Have targets for numerical accident probability or rate been agreed for each type of potential accident?
- s) Have targets for numerical accident probability or rate been agreed for elements of the accident sequence?
- t) Have targets (quantitative or qualitative) been allocated down to sub-system functional level?
- u) Have quantitative hazard rate targets been apportioned separately to the random and systematic failure modes?
- v) Has the potential effects of common cause failures been assessed?
- w) Have random hazard rate targets been apportioned to the lower level functions of the system?
- x) Have Safety Integrity Levels been defined for the systematic elements?
- y) Have Safety Integrity Levels been apportioned to lower level functions according to agreed rules (see Chapter 9)?

- z) Have the targets and criteria developed from the above been adequately recorded and reported in the Hazard Log? \*
- aa) In carrying out the Safety Assessment, it is necessary to compare the random targets with those predicted for the random elements. Is the comparison satisfactory? \*
- ab) For the Safety Assessment of the systematic elements, it is necessary to audit the design against the tolerable levels of risk, the agreed rules for Safety Integrity Levels and the design techniques. Is the design acceptable? \*

#### D.6.5 Assessment checklist: Customer acceptance and validation

Checklist for Safety Assessor:

- a) Does the Safety Plan contain an element relating to a test and acceptance programme?
- b) Are the safety features of the design identified for acceptance tests?
- c) Do you have any comments or recommendations concerning the adequacy of the test programme? \*
- d) Have the results of the safety test and acceptance programme been recorded and reported in the Hazard Log?
- e) Are the results satisfactory? \*
- f) Are there any shortcomings or outstanding items? \*
- g) Is the level of test coverage adequate?

#### D.6.6 Assessment checklist: Site trial/pilot scheme

Checklist for Safety Assessor:

- a) Does the Safety Plan contain requirements for the conduct of Site Trial?
- b) Does the Safety Plan contain requirements for the conduct of a Pilot Scheme?
- c) Are the safety features of the system design identified for Site Trial purposes?
- d) Are the safety features of the system design identified for Pilot Scheme purposes?
- e) Do you have any comments regarding the adequacy of the Site Trial to demonstrate the safety features? \*
- f) Do you have any comments regarding the adequacy of the Pilot Scheme to demonstrate the safety features? \*
- g) Has an incident or defect reporting system been set up for the Site Trial?
- h) Is the trial covered by a Safety Certificate?
- i) Is the system being used with the constraints of the Safety Certificate?
- j) Are all necessary support arrangements in place?

**D.6.7 Assessment checklist: In-service support**

Checklist for Safety Assessor:

- a) Has support of the system in service been addressed during Requirements Definition?
- b) Has support of the system in service been addressed during Design and Development?

This page left intentionally blank