



## FIRE RISK ASSESSMENT STUDY FOR A HIGH SPEED TRAIN

**By Paul Mann – Principal RAMS and Systems Assurance Advisor**



*Mr. Mann is a graduate in Physics from Leeds University, a Chartered Engineer via the Institute of Mechanical Engineers and a Fellow of the UK Safety & Reliability Society. He has worked as a RAMS consultant to the railway industry both in the UK and Internationally for Twelve of his Twenty Five year career. He is currently the Managing Director of PMSC Limited and has successfully negotiated and completed RAMS contracts for a range of railway contractors and operators including: Alstom, Bombardier, Siemens, Areva T&D, Singapore Land Transport Authority, NEC, Kawasaki Heavy Industries, Toshiba, Mitsubishi, London Underground, Railtrack and Network Rail.*

### CONTENTS OF PAPER

<b>Section 1.0</b>	<b>Background.....</b>	<b>2</b>
<b>Section 2.0</b>	<b>Overview of Typical Safety Design Features .....</b>	<b>2</b>
<b>Section 3.0</b>	<b>Some Background on Fault and Event Trees .....</b>	<b>2</b>
<b>Section 4.0</b>	<b>Typical Structure of Event Tree .....</b>	<b>8</b>
<b>Section 5.0</b>	<b>Assignment of Consequence Categories .....</b>	<b>11</b>
<b>Section 6.0</b>	<b>Some Useful Rules for the Assignment of Consequence Categories</b>	<b>13</b>
<b>Section 7.0</b>	<b>A worked example for a Fire in a Luggage Rack.....</b>	<b>15</b>
<b>Section 8.0</b>	<b>The Calculation of Risk.....</b>	<b>19</b>
<b>Section 9.0</b>	<b>Useful References .....</b>	<b>21</b>
<b>Section 10.0</b>	<b>Some Useful Data Sources for QRA Purposes.....</b>	<b>23</b>

### Abstract

***It has been said that passengers travelling on high-speed trains are entitled to expect the highest standard of care in terms of safety. Fire should always be a major consideration in the provision of rolling stock and railway systems and as such this paper proposes an outline methodology to predict the frequency of fires on high speed trains and more specifically a methodology to be able to allow designers to assess the benefit of various fire safety provisions to be able to evaluate whether individual provisions are reasonably practicable and in an overall sense whether the residual risk of travelling on a high speed train is As Low As Reasonably Practicable, ALARP. The modelling is presented in a generic way and is not directly applicable to any particular project, although the overall approach is one, which the author has used to great success on real projects in Asia.***



## Section 1.0 Background

This paper is a generic study of the process involved in developing a Quantified Risk Assessment (QRA) for a typical high-speed train. The QRA has been developed using state of the art modelling techniques making use of an integrated Fault and Event Tree approach.

Typically, the first task in generating a fire QRA is to identify the initiating event scenarios to be modelled. In the case of the current model some example scenarios modelled have been listed below:-

### Fires starting inside the Train

- Fire in a luggage rack
- Fire in a toilet
- Fire in an Electrical Cabinet on the train
- Fire in the cab or behind the driver

### Fire starting outside the Train

- Fire on the train under-frame, developing from a Main Transformer
- Fire on the train under-frame, developing from a Traction Converter Inverter
- Fire on the train under-frame, developing from a stuck brake

## Section 2.0 Overview of Typical Safety Design Features

In the QRA modelling we are looking to take appropriate numerical credit for the various fire protection features, which may be present in the design and to test these features in terms of their adequacy via the ALARP argument. Typically, on a high speed train the following features may be present in the design, use of approved fire tested materials in the train (eg. Materials certified to meet the requirements of BS6853 and BS 476 parts 6 and parts 7); use of appropriately located smoke detectors; (usually in fresh air intakes and inside saloons and toilets) use of fire wires (usually on the under-frame equipment); and the use of strategically placed hand held fire extinguishers for use by train master and passengers. Other design features could include provision of alternative escape ways for the driver in case he is trapped in the cab by a fire and cannot leave by the normal route.

The trick in developing a successful QRA model is to find a framework for the fault and event tree modelling which allows consideration of all the various possible safety features which could be present and allow a prediction of their worth in combating the initiation and subsequent development of a fire.

## Section 3.0 Some Background on Fault and Event Trees

### 3.1 Event Trees

Event trees diagrammatically illustrate a sequence of events modelling accident scenarios. An example event tree has been presented below (see Figure 3.1). The “nodes” along the top of the event tree represent questions with a YES or NO answer, the convention being the downward branch representing the “NO” answer and the horizontal branch, representing the “YES” answer. This can also be termed as failure or success, respectively.



Outcome 5 in figure 3.1 derived using the following Boolean expression

Outcome 5 Frequency = Union of the success terms for the event TOP with failure of system X and success of system Y and system OP. The Boolean expression for this is written as Outcome 5 =  $TOP \cdot X \cdot Y' \cdot OP'$

Please note that the dash next to the terms Y and OP indicates that these are success terms rather than failure terms. Success terms are referred to as PATH sets whilst failure terms are referred to as PATH sets. It should also be noted that sometimes instead of using dashes to represent PATH sets a small bar will be placed on top of the symbol to represent success.

The Frequency of Outcome 5 is then derived as follows:-

Frequency of Outcome 5 in the event Tree = Frequency of TOP event multiplied by the Probability that event X fails multiplied by the probability that event Y is successful multiplied by the probability that event OP is successful this is shown mathematically below:-

$$\text{Frequency of Outcome 5} = F(\text{TOP}) \times P(x) \times (1-P(Y)) \times (1-P(OP))$$

It should be noted that the Event Trees are normally designed such that the success branch will produce the least consequences and the failure branch to produce the most consequences.



PMSC Limited Paper on Generic Approach to Fire QRA for High Speed Trains

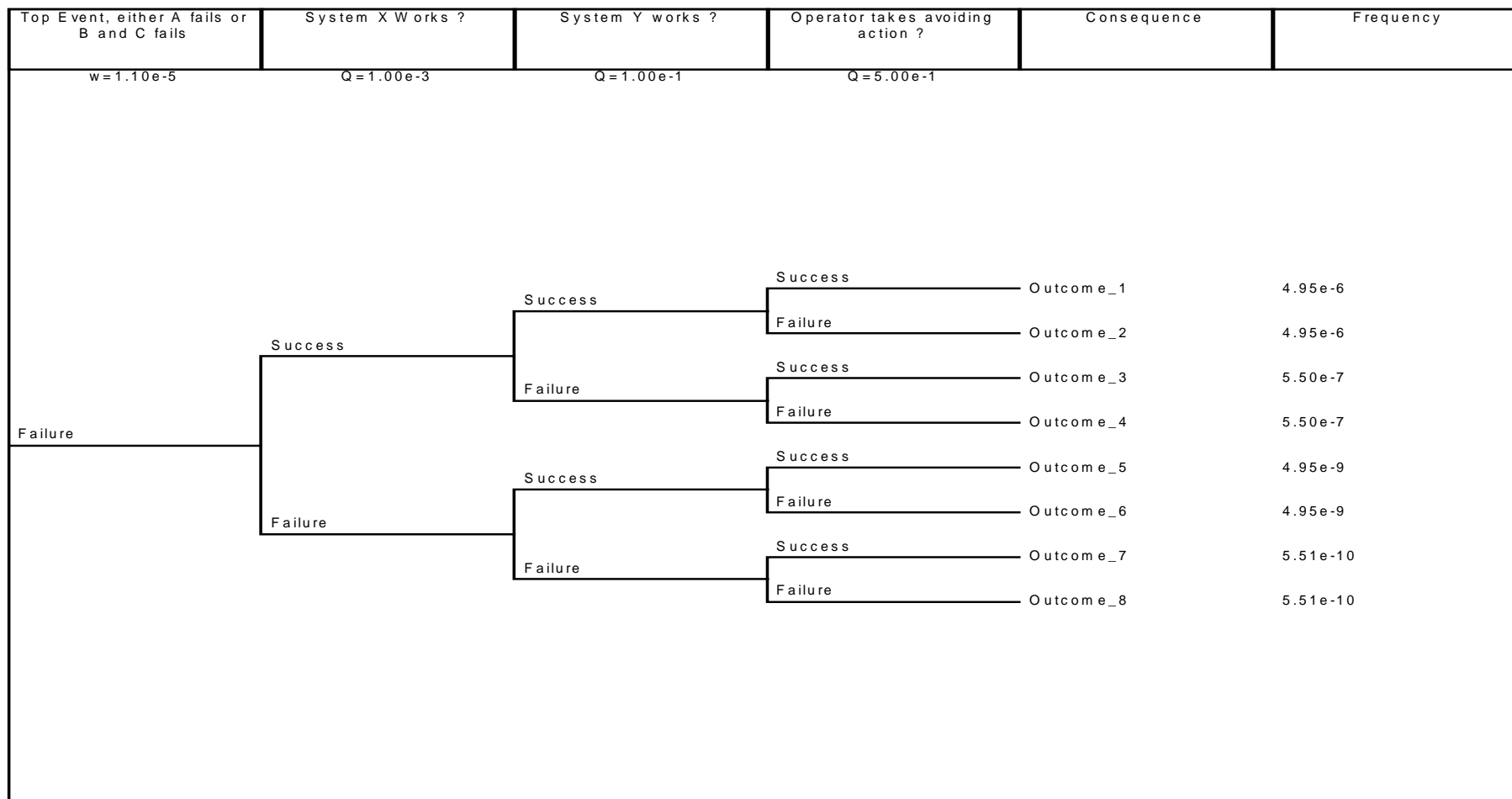
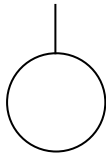
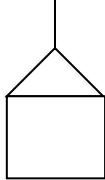
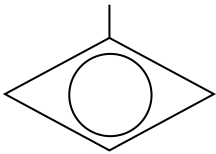
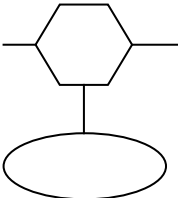


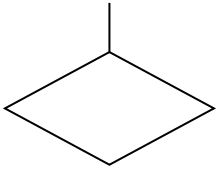
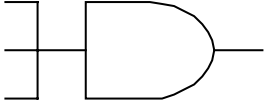
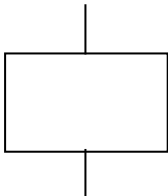
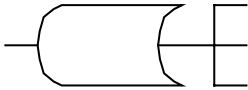
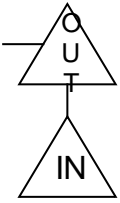
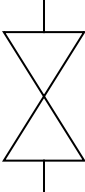
Figure 3.1: Generic Event Tree Structure Illustrating the typical event tree format

### 3.2 Fault Trees

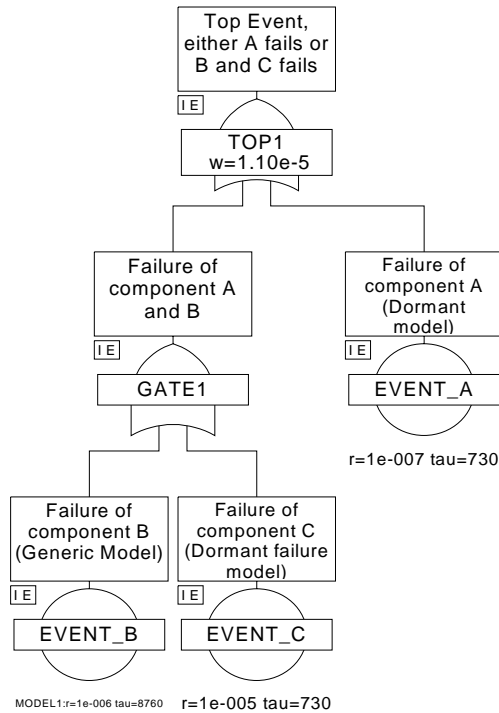
Fault trees are generally used when constructing a quantified risk assessment to quantify the hazards identified in the HAZOP and Hazards Log, to more accurately determine safety critical hazards and to assure that the (As Low As Reasonably Practicable, ALARP) principle has been satisfied in relation to the residual risk. The Fault Tree will generally identify equipment or software components that indicatively affect the hazards risk, thereby providing a tool for analysing the total effect of failure rates and Mean Time To Repair (MTTR) of components and their relationship to hazard consequences and in summary their effect on the top event.

The table 3.1 below presents an indication of the typical symbols and their meanings, to be used in fault trees presented in a typical risk assessments

 <p>Basic Event The circle describes a basic event that requires no further development.</p> <p>Frequency and mode of failure of items so identified are derived from empirical data. It should be noted that if failures are revealed the Fault Tree + RATE model will be utilised requiring the failure rate of the component and the repair rate. If failures are un-revealed then the Fault Tree + DORMANT model shall be adopted requiring the failure rate and the testing interval of the component. It should be further noted that each of the components modelled in the QRA will be given a coding name which represents their component type and failure mechanism, this will be agreed prior to the QRA development by the event nomenclature table.</p>	 <p>Switch The house event is used as a switch to include or eliminate parts of the fault tree. Effectively True or False to those parts in the system. If a house event is AND'ed with a part of a tree it has the effect on including the other branch of the tree, if it is OR'ed then the other branch is effectively discounted or switched off.</p>
 <p>Basic Event Indicates a sub tree exists, but the sub tree was evaluated separately and the quantitative results inserted as a basic fault event</p>	 <p>Inhibit Gate Describes a relationship between one fault and another. The input event directly produces the output event if the indicated condition is satisfied.</p>

	<p><b>Basic Event</b> The diamond describes a fault event that is considered basic in a given fault tree. The possible causes of the event are not developed because the event is of insufficient consequence or the necessary information is unavailable. It is possible that such events might be included for information but not actually explicitly modeled as part of the numerical analysis.</p>		<p><b>AND Gate</b> Describes the logical operation whereby the existence of all input events is required to produce the output event. If the inputs are event A and event B then the solution at the AND gate is the product of event A and event B i.e. Both must fail for the gate to be satisfied.</p>
	<p><b>Combination Event</b> The rectangle identifies an event that results from the combination of basic events through the input logic gates</p>		<p><b>OR Gate</b> OR gates define the situation whereby the output event will exist if one or more of the input events exist. If the inputs are event A and event B then the solution at the OR gate is that either event A or event B can fail. Additionally, voting gates (which utilise the OR symbol) will be used to represent areas where failure of combinations such as one out of two or two out of three or three out of four failures can occur.</p>
	<p><b>Transferred Event</b> The triangles are used as transfer symbols. A line from the apex of the triangle indicates a transfer in, a line transfer out. Transfers in can be used to avoid unnecessary duplication of large sections of fault trees that might appear in several places – for example fault trees modelling failure of electrical supplies might be used in several places in the overall QRA model.</p>		<p><b>NOT Gate</b> NOT gates define the situation whereby the logical state of an event is reversed. The use of NOT gates will be limited, but their existence needs to be highlighted for completeness.</p>

**Table 3.1 Typical List of Fault Tree Symbols**



**Figure 3.2 An Example Simplistic Fault Tree**

The above fault tree (figure 3.2) represents a simplistic tree where the failures, which satisfy the top event are either Component A fails or Component B and C fail. Hence, we say that the minimum Cut Sets are A and BC, i.e. there are 2 minimum Cut-sets one of a single order i.e. A and one of order two i.e. BC, this illustrates that a failure of A will directly lead to the top event, or that a failure of both B and C would lead to the top event.

## Section 4.0 Typical Structure of Event Tree

As discussed above, when developing an Event tree it is important to develop the nodal questions, which the event tree will model. For a typical high speed train the following nodes or key questions are proposed:-

- Event Tree Node 1: Where is the fire?
- Event Tree Node 2: Where is the train at the time of the fire (route could be in tunnel or on viaducts)
- Event Tree Node 3: Is the train at full line speed at time of fire?
- Event Tree Node 4: Do the train fire detection systems work?
- Event Tree Node 5: Does the driver take correct action once fire is discovered?
- Event Tree Node 6: Do the passengers successfully evacuate the car affected by the fire?
- Event Tree Node 7: Does the fire escalate?
- Event Tree Node 8: Does the train stop in a place of safety?
- Event Tree Node 9: Can affected passengers safely egress from the train?
- Event Tree Node 10: Can the passengers be recovered safely by the Train Operating Company?

In terms of an example event tree structure please refer to figure 7.1, each of these key nodes is discussed further in turn:-

### 4.1 Event Tree Node 1: Where is the fire?

This node models the initiating event, the specific location of the fire. Typically, in high speed train applications once is concerned to model typical internal fires eg. fire in luggage rack or fire in toilet and also fires which may occur outside the train on the under-frame. Usually, only the high-energy components are considered for the initiation of a fire such as the Main Transformers or Converter Inverters but other locations such as Brakes could also be considered as fire cases.

### 4.2 Event Tree Node 2: Where is the train at the time of the fire?

The provisions for escaping from a train on fire may well be different if the train is stopped in a tunnel as opposed to being stopped for example on a viaduct. Therefore it is important to be able to differentiate. Hence the fraction of the route in tunnels is a useful metric to be able to quote.

### 4.3 Event Tree Node 3: Is the train at full line speed at time of fire?

On high-speed routes the full line speed maybe in excess of 280 km/hr however there will be degraded modes (perhaps where the Automatic Train Control) is inoperable which mean that speed restrictions might be imposed. It is important in the event tree to be able to differentiate between these two scenarios. Usually, the percentage of time spent at high speed can be estimated for use in the event tree.

### 4.4 Event Tree Node 4: Do the train fire detection systems work?

This node can usually be modelled by a fault tree where the combined worth of the detection systems eg. Smoke detectors in internal fire scenarios and possibly a



combination of smoke detectors or fire wires in under-frame scenarios. It is usually important to make assumptions about the control systems in these fault trees ie. The fault tree would model not just the detectors but also any common elements in the control system logic. It is usual as a conservatism to only claim the detection system in the car where the fire starts, that is to say claims for detectors in adjacent saloon cars are conservatively neglected. See Typical Fault Tree as figure 7.3.

**4.5 Event Tree Node 5: Does the driver take correct action once fire is discovered?**

In order for the driver to act correctly the detection system must work properly, this sets some structure to the event tree. Usually on high speed routes the correct action for the driver to take will be to call the Central Operational Control Room for them to identify the place of safety for him to stop the train, this could be at the next station or an alternative location.

**4.6 Event Tree Node 6: Do the passengers successfully evacuate the car affected by the fire?**

In the event of a fire in a saloon the passengers should be moved into adjacent cars and any fire barrier doors closed. The Train Master (if one is present on the train) will assist with this evacuation process. Alternatively the train driver may initiate a message over the Passenger Information systems.

**4.7 Event Tree Node 7: Does the fire escalate?**

In many fire cases the spread of fire may be prevented by the use of hand held fire extinguishers or other actions by Train Master and or Passengers. In other cases where the design has made such provision, automatic fire suppression systems can be initiated to extinguish fires. It should be noted that such automated systems are usually only found on locomotive systems and are not usually provided inside the cars of electrical multiple units or other high-speed trains. See Typical Fault Tree as figure 7.2.

**4.8 Event Tree Node 8: Does the train stop in a place of safety?**

Some high-speed rail systems have automatic station stopping systems, which minimise the potential for a train to come to rest in an incorrect location. However, in emergency situations where a train may not stop at a station but may stop at some alternative location such as an emergency escape way if stopping in a tunnel, it may be that the train could come to rest at an incorrect location. This may be either due to driver error or other human errors committed in the Central Operational Control Room. Additionally, the fire may result in failure of systems such as brakes thus resulting in an increased stopping distance and potential over run.

**4.9 Event Tree Node 9: Can affected passengers safely egress from the train?**

In the eventuality that the train comes to rest, this node models whether the passengers can accomplish egress from the train with out further incremental



equivalent fatalities. It is essential that passengers are appropriately marshalled once they have left the train so that consequential fatalities and or injuries can be avoided.

**4.10 Event Tree Node 10: Can the passengers be recovered safely by the Train Operating Company?**

The fact that passengers can be safely moved off the train does not necessarily mean that they are fully recovered. For example a train may stop between stations and thus, passengers may not be recovered, until they are recovered to a station stop, this implies further action by the train operating company.

### Section 5.0 Assignment of Consequence Categories

At each end point of the event tree (a fully developed event tree with N nodes has  $2^{(N-1)}$  end points, though it should be noted that event trees are rarely fully developed) a consequence category should be assigned. Guidance on risk ranking criteria in EN50126 can be useful here. Consequences are assigned in terms of fatalities but more sophisticated QRA's now utilise the concept of Equivalent fatalities which allows the combined consideration of Fatality, Major Injuries and Minor Injuries within the same QRA model. Normally, the convention used to calculate Equivalent Fatalities is as follows:-

$$\text{Equivalent Fatalities} = \text{Actual Fatalities} + \text{Major Injuries}/10 + \text{Minor Injuries}/200$$

The above is by no means a “tablet of stone” and may vary between different projects.

Some example Consequence Categories have been illustrated below from EN50126.

LIKELIHOOD	DEFINITION	FREQUENCY GUIDE
Frequent	Continually occurs during operational life-cycle	100 /year
Probable	May occur a few time during life-cycle	10 /year
Occasional	May occur several times during operational life of system	1 /year
Remote	May occur at some time in the system life-cycle	1 / 10 years
Improbable	Unlikely to occur during operational life	1 / 100 years
Incredible	Extremely unlikely to occur	1 / 1000 years

**Table 5.1 Typical Frequency Matrix**

SEVERITY	PERSONNEL	SYSTEM	ENVIRONMENTAL
Disastrous	Not defined in EN50126	Not defined in EN50126	Not defined in EN50126
Catastrophic	Multiple deaths and/or widespread fatal illness	Loss of a critical physical asset. Leading to failure of a critical system such as signalling potentially leading to catastrophic disruption to the running of the Railway	Significant, prolonged or widespread damage to a habitat or species
Critical	Single death and/or multiple severe injuries or occupational illnesses	Major system loss, mission failure. Major disruption caused.	Major damage or medium-term damage of a habitat or species
Marginal	Single severe injury or occupational illness and / or multiple minor injuries	System damaged, lost functionality. Interference with non critical systems	Small-scale, short-term damage to a habitat or species
Negligible	Minor injury or occupational illness	Minor damage to system. System not functioning as intended however not affecting any other system	Minor local damage to a habitat or species

**Table 5.2 Typical Severity Matrix**



SEVERITY	NEGLIGIBLE	MARGINAL	CRITICAL	CATASTROPHIC
OVERALL FREQUENCY				
FREQUENT	B	A	A	A
PROBABLE	C	B	A	A
OCCASIONAL	C	B	B	A
REMOTE	D	C	B	B
IMPROBABLE	D	D	C	C
INCREDIBLE	D	D	D	D

Tolerability Key:

A = Intolerable.  
 B = Undesirable and only accepted when risk reduction is impracticable.  
 C = Tolerable with endorsement  
 D = Tolerable.

**Table 5.3 Typical Tolerability / Risk Matrix**



## **Section 6.0 Some Useful Rules for the Assignment of Consequence Categories**

A consequence category from the tables above has been assigned at the end of every event tree end point. The rules that have been used in assigning these consequences are described in out line below, the consequence categories can be seen at the end point of each sequence in the event trees:

Rule 1: Where either the driver successfully takes prompt and correct action or passengers can successfully evacuate to adjacent cars, and passengers can accomplish safe egress, “negligible “ consequences are assigned.

Rule 2: Where either the driver successfully takes prompt and correct action or passengers can successfully evacuate to adjacent cars, but passengers cannot accomplish safe egress, “ Marginal” consequences are assigned.

Rule 3: Where passengers in cars #1 and #12 fail to fight the fire, “ Disastrous” consequences are assigned, excepting the following cases:- it should be noted that whilst EN50126 does not cite a disastrous consequence category some customers have included such criteria in their specifications.

a) under circumstances where the driver has taken prompt and correct action, then “ Catastrophic ” consequences are assigned on the basis that even though the fire may be extinguished by the hand held extinguishers there may be injuries and possible fatalities arising due to smoke inhalation.

b) Under circumstances where even though the driver may not have taken prompt and correct action and the train may not have stopped at a place of safety because either the passengers or the Train master may have managed to successfully prevent the escalation of the fire only “Critical” and NOT Catastrophic consequences are assigned on the basis that some limited numbers of fatalities or injuries may have been sustained whilst fighting the fire.

Rule 4: In circumstances where the driver fails to take prompt and correct action, the train fails to stop at a place of safety, and the fire is in cars #2 to #11, “ Catastrophic” consequences conservatively are assigned.

Rule 5: Where the driver fails to take prompt action and the fire is in cars #1 or car #12, but passengers or Train Master are successful in delaying the escalation of the fire and the train stops at a place of safety and safe egress is accomplished then “ Negligible” consequences are assigned. In cases where all the above apply, with the exception of safe egress not being accomplished then “ Marginal” consequences are assigned.

Rule 6: Where the automatic smoke detection system fails, “ Disastrous” consequences are conservatively assigned. It should be noted that whilst EN50126 does not cite a disastrous consequence category some customers have included such criteria in their specifications.



## **PMSC Limited Paper on Generic Approach to Fire QRA for High Speed Trains**

Rule 7: ONLY where the automatic smoke detection system works but the train fails to stop at a place of safety OR the driver fails to take prompt action IF the driver can escape from the cab, it is assumed he will assist with the orderly evacuation and as a result reduced consequences will result i.e. consequences in these circumstances will be assigned as Serious rather than Critical. It should be noted that calculations included in the main text have shown that the longest time to reach a place of safety is shorter than the 15 minutes fire barrier provided by the wall ends in each of the cars.



## Section 7.0 A worked example for a Fire in a Luggage Rack

The event tree and two fault trees presented below represent an edited version of an actual high-speed rail risk assessment with sanitised data to protect client confidentiality. The structure of the event tree has been carefully edited to ensure that the event tree reflects the logical development of a luggage rack fire.

Initially, only fires where the train is about to enter a tunnel are considered in the event trees, hence only a single branch is used for node 1. Nodes 2,3 are fully developed with success and failure logic in the event tree. However, node 4 is set as a “null” on the failure branch of node 3 since if the fire is not detected by the smoke detection system it is conservatively assumed that the driver cannot take prompt and correct action unless the Train Master alerts him.

At present no claim for the Train Master alerting the driver has been taken although in the case of smoke detection systems failure there would still be the opportunity for the passengers, to alter the Train Master to smoke arising from the luggage rack and for the Train Master to alert the driver using the on board communication systems.

The various other smoke detectors are claimed by means of fault trees, which are interfaced into the failure branches of the event tree nodes this provides for a fully interfaced Fault and Event Tree model.

Node 5 is fully developed in success and failure logic except on the failure branch of node 3, indicating that if the fire is not detected by the smoke detection system it has been assumed that the passengers will not be alerted to move into adjacent cars.

Node 6 is set as a “null” on the success path of node 5 since if passengers successfully evacuate to an adjacent car then they will not be available to fight any fire with hand held extinguishers. This is slightly conservative in the sense that although passengers may have evacuated the fire could be fought by the Train Master alone, although this has not been claimed. The exception to the above being, when the fire is in car # 1 or car #12 where the passengers are trapped by the fire and have no option but to fight it or escape via the windows if the train is stopped.

The node 8 is undeveloped on the failure branch of node 7, since if the train fails to stop at a place of safety it is judged that the question of the passengers accomplishing safe egress is a moot point.



Where is the fire ? (Luggage Rack)	Where is the Train at the Time of the Fire?	Train at Full Line Speed?	Do Train Fire Detection Systems Work?	Does Driver Take Correct Action once fire is discovered?	Do Passengers Successfully Evacuate Car affected by Fire?	Does the Fire Escalate?	Does Train Stop in a Place of Safety?	Can Passengers Safely Egress from Train?	Consequence	Frequency	Probability
w=2.000e-2 <small>FIRE IN LUGGAGE RACK</small>	Q=2.000e-1 <small>ET1_LOCATION</small>	Q=1.000e-1 <small>ET1_SPEED</small>	Q=1.143e-4 <small>#ET1_SD_FAIL_LLR</small>	Q=3.000e-2 <small>ET1_DRIVER</small>	Q=8.333e-2 <small>ET1_PASS_EVAC</small>	Q=1.081e-2 <small>#TM_PLR_FIRE_EXTINGUISHER</small>	Q=5.000e-1 <small>ET1_POS</small>	Q=1.000e-1 <small>ET1_EGRESS</small>		4.000e-3	2.000e-1
Page 3			Page 2								
Failure:Fire in Luggage Rack on Train  Failure:Tunnel (No ER)  Failure:30kmh	Success:300kmh		Success	Success	Success:2-11	Null	Null	Success	Negligible	2.881e-3	1.440e-1
				Failure	Failure:1+12	Success	Null	Failure	Marginal	3.201e-4	1.600e-2
						Success	Null	Success	Negligible	2.590e-4	1.295e-2
						Failure	Success	Success	Marginal	2.878e-5	1.439e-3
						Failure	Failure	Success	Negligible	1.415e-6	7.075e-5
							Failure	Failure	Marginal	1.572e-7	7.861e-6
							Failure	Null	Critical	1.572e-6	7.861e-5
						Success:2-11	Null	Success	Negligible	4.454e-5	2.227e-3
						Failure:1+12	Success	Failure	Marginal	4.949e-6	2.475e-4
						Success	Success	Success	Catastrophic	4.949e-5	2.475e-3
						Failure:1+12	Failure	Success	Negligible	4.006e-6	2.003e-4
						Failure	Failure	Failure	Marginal	4.451e-7	2.225e-5
						Failure	Null	Null	Critical	4.451e-6	2.225e-4
						Failure	Null	Null	Disastrous	9.725e-8	4.862e-6
						Success:2-11	Null	Null	Disastrous	4.113e-7	2.057e-5
						Failure:1+12	Success	Failure	Negligible	3.201e-4	1.600e-2
						Success	Success	Success	Marginal	3.556e-5	1.778e-3
						Failure:1+12	Failure	Success	Negligible	2.878e-5	1.439e-3
						Failure	Null	Null	Marginal	3.198e-6	1.599e-4
						Success:2-11	Null	Success	Critical	3.494e-7	1.747e-5
					Success	Success	Success	Negligible	4.949e-6	2.475e-4	
					Failure:1+12	Failure	Failure	Marginal	5.499e-7	2.750e-5	
					Success	Success	Success	Catastrophic	5.499e-6	2.750e-4	
					Failure:1+12	Failure	Success	Negligible	4.451e-7	2.225e-5	
					Failure	Failure	Failure	Marginal	4.945e-8	2.473e-6	
					Failure	Null	Null	Critical	4.945e-7	2.473e-5	
					Failure	Null	Null	Disastrous	1.081e-8	5.403e-7	
					Failure	Null	Null	Disastrous	4.570e-8	2.285e-6	

Figure 7.1: Typical Event Tree Structure (Fire In Luggage Rack)



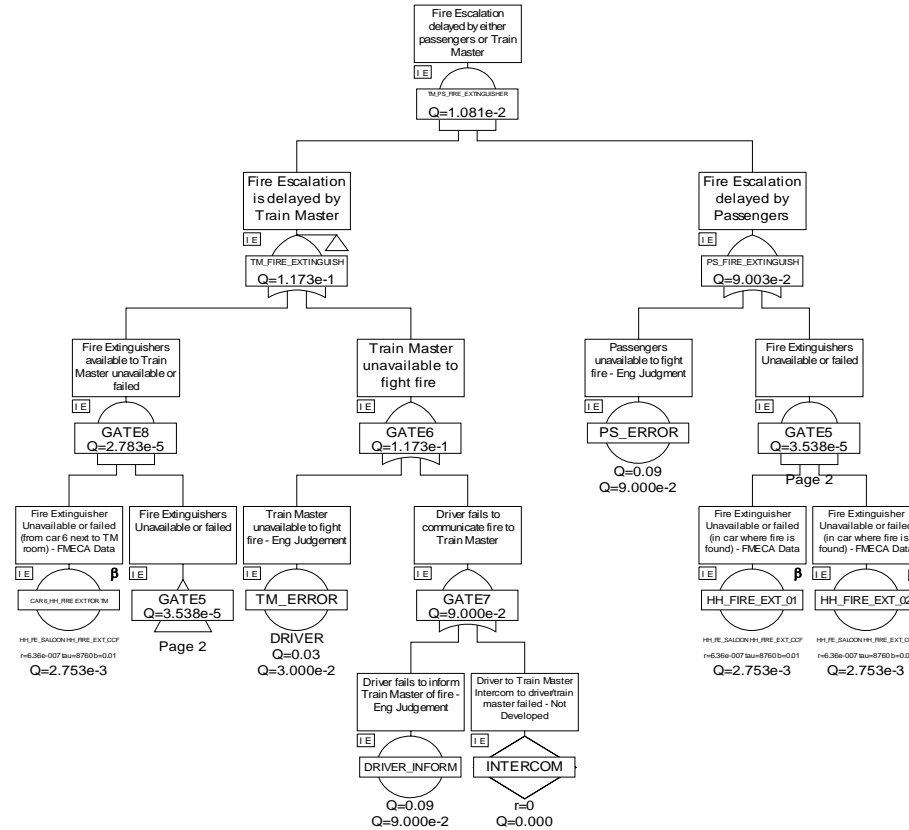


Figure 7.2: Typical Fault Tree Structure (Fire Escalation Delayed)

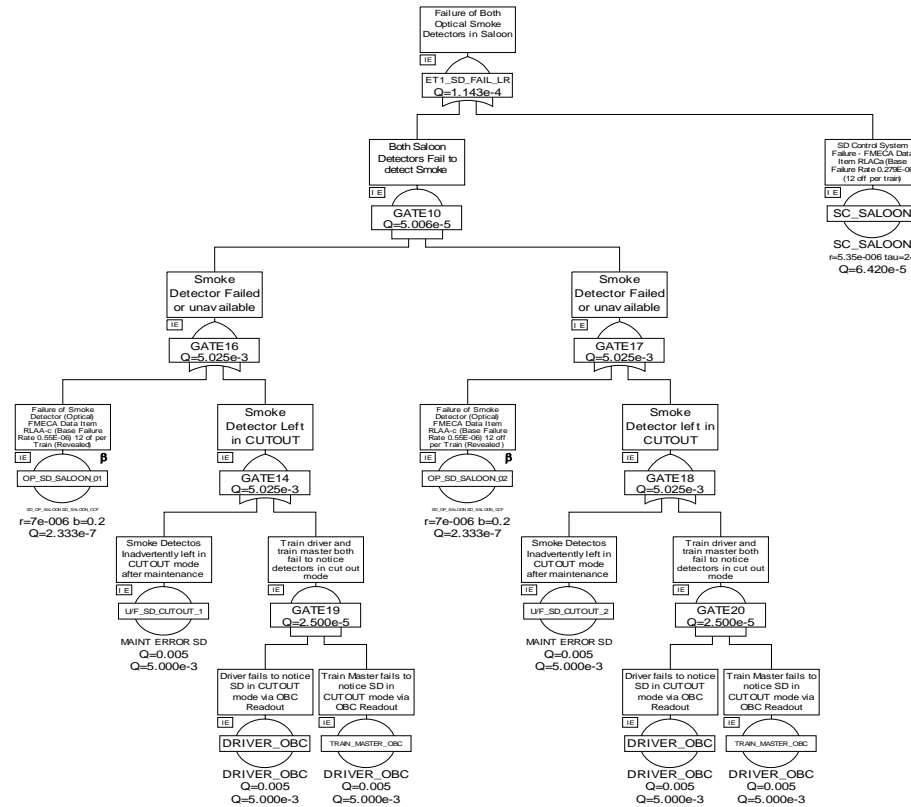


Figure 7.3: Typical Fault Tree Structure (Failure of Smoke Detection Systems in Saloon)



## Section 8.0 The Calculation of Risk

The results of Fault and Event Tree analysis are usually the summated products of the combination of derived frequency and equivalent fatality consequence for each consequence category. It is sometimes useful when using the Fault Tree + software to enter weighting factors to act as multipliers to normalise the eventual risk answers to become % of the allowable target.

For example, if the target for a rolling stock system is say 10% of the overall system target and this is set as 0.007 Equivalent Fatalities per 1.0E+09 Km then by using the following weighting factor

Weighting Factor=(No of Equivalent Fatalities/No of Passenger Km per year)

Where No of Equivalent Fatalities is derived from table 8.1 and the No of Passenger Km per year is estimated for the specific route under consideration to be say 15.0E+09

Using the consequence table above and setting some fatality, major injury and minor injury bands as guidelines we arrive at the derived number of Equivalent fatalities for each consequence category presented in the right hand column of table 8.1

The weighting factors can then be used directly in the Fault Tree + software to calculate % of target used for each consequence category.



**PMSC Limited Paper on Generic Approach to Fire QRA for High Speed Trains**

SEVERITY	GUIDANCE	Number of			EQUIVALENT FATALITIES	WEIGHTING FACTOR % RISK
		FATALITIES	MAJOR INJURY	MINOR INJURY	EF	WF=(EF/15/0.007)*100%
Catastrophic	Multiple deaths and/or widespread fatal illness	>1 but <say 500	5 to 50	>50 but say <500 the total no passengers per train	$(500+1)/2$ + $(50-5)/2/10$ + $(500-50)/2/200$ <b>=253.875</b>	241,785.7143
Critical	Single death and/or multiple severe injuries or occupational illnesses	1	>1 but less than 5	5 to 50	1 + $(5-1)/2/10$ + $(50-5)/2/200$ <b>=1.3125</b>	1,250
Marginal	Single severe injury or occupational illness and / or multiple minor injuries	0	1	>1 but less than 5	0 + $1/10$ + $(5-1)/2/200$ <b>=1.1E-01</b>	104.76
Negligible	Minor injury or occupational illness	0	0	1	0 + $0/10$ + $1/200$ <b>=5.0E-03</b>	4.7619

**Table 8.1 Calculation of Weighting Factors using Equivalent Fatalities**



**Section 9.0 Useful References**

Topic Area	International Standards/Data Sources
FMECA	<ul style="list-style-type: none"> <li>• Military Standard 1629</li> <li>• IEC Publication 812'Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Criticality'.</li> </ul>
HAZOP	<ul style="list-style-type: none"> <li>• MIL-STD-882B: 'System Safety Management',</li> <li>• prENV50126: 'Railway Applications – The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS)'</li> <li>• DEF STAN 00-58'Hazop Studies on Systems Containing Programmable Electronics'</li> <li>• "Hazop and Hazan" by T Kletz (UK) Institution of Chemical Engineers 3<sup>rd</sup> Edition 1992.</li> <li>• Railtrack Yellow Book</li> </ul>
FTA and ETA	<ul style="list-style-type: none"> <li>• NUREG-0492 'Fault Tree Handbook' D F Hassel, N H Roberts, W E Vesely, and F F Goldberg US Nuclear Regulatory Commission</li> <li>• Reliability and Risk Assessment by J.D Andrews and TR Moss ISBN 0-470-23345-1, Chapter 7 Fault Tree Analysis.</li> <li>• Combined FTA/ETA modeling tool is Fault Tree + (Currently version 9)</li> </ul>
Reliability Analysis (includes analysis and demonstration)	<ul style="list-style-type: none"> <li>• IEC 61508 - Functional Safety: Safety-Related Systems Part 2 and 6</li> <li>• MIL-STD-785B: 'Reliability Program for Systems and equipment Development and Production</li> <li>• MIL-STD-756: ' Reliability Modeling and Prediction'</li> <li>• MIL-STD-2173: ' Reliability Centred Maintenance</li> <li>• MIL-HDBK-217F: 'Reliability Prediction of Electronic equipment',</li> <li>• DEF STAN 00-40: 'Reliability and Maintainability Parts 1-8',</li> <li>• DEF STAN 00-43: 'Reliability and Maintainability Assurance Activity'.</li> </ul>



Topic Area	International Standards/Data Sources
	<ul style="list-style-type: none"> <li>• International Electrotechnical Commissions Standard – 60300 – Dependability Management</li> <li>• International Electrotechnical Commission Standard – 60571, Part 3 – Electronic Equipment Used on Rail Vehicles, Components, Programmable Electronic Equipment and Electronic System Reliability</li> <li>• International Electrotechnical Commissions Standard 60605, Equipment Reliability Testing</li> <li>• BS Euro Norm 50126, 1999, Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)</li> <li>• Euro Norm 50129, 1998, Railway Applications – Safety Related electronic systems for Signalling.</li> <li>• MIL-STD-471A – Military Standard Maintainability Verification / Demonstration / Evaluation.</li> </ul>
Software SIL Analysis	<ul style="list-style-type: none"> <li>• IEC 61508 Parts 3 and Parts 6, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related systems Part 3 : Software Requirements, Part 6 : Guideleines on the applications of parts 2 and 3.</li> <li>• RIA 23, BRB/LU LTD/RIA Technical Specification Number 23 1991, Safety Related Software For Railway Signalling – Consultative document. (this has now been largely superceeded by the requirements as set out in IEC 61508)</li> <li>• prEN 50128, Draft European Standard, Railway Applications – Software For Railway Control and Protection Systems.</li> </ul>
Human Factors	<ul style="list-style-type: none"> <li>• Human Reliability Assessors Guide Book</li> <li>• A Guide to Task Analysis</li> <li>• NUREG 1278 Swaine &amp; Guttman</li> <li>• Papers by Williams on HEART</li> </ul>
Fire Analysis	<ul style="list-style-type: none"> <li>• BS6853 1999, Code of Practice for Fire Precautions in the design and construction of passenger carrying trains</li> <li>• BS476, Fire tests on Buildings Materials and Structures, Part 6 Method of Test for Fire Propagation for Products</li> <li>• BS476, Fire tests on Buildings Materials and Structures, Part 7 Method of Test to determine the classification of the surface spread of flame of products</li> <li>• NFPA 130, Standards for Fixed Guideway Transit and Passenger Rail Systems 2000 Edition.</li> </ul>



## Section 10.0 Some Useful Data Sources for QRA Purposes

Data Source	Comments
OREDA 92	<ul style="list-style-type: none"> <li>Mainly used in the offshore oil and gas sector for equipment reliability.</li> </ul>
Mil Hdbk 217	<ul style="list-style-type: none"> <li>Electronics reliability assessment</li> </ul>
IEEE-500	<ul style="list-style-type: none"> <li>Mechanical and electrical component reliability database compendium</li> </ul>
NPRDS	<ul style="list-style-type: none"> <li>Non Electronics Parts Reliability Database</li> </ul>
Mil Hdbk 472	<ul style="list-style-type: none"> <li>Maintainability data handbook</li> </ul>
PMSC in house	<ul style="list-style-type: none"> <li>Data base of man made accidents around the world since the 1700 hundreds.</li> </ul>

### About PMSC Limited

PM Safety Consultants is a specialist Systems Assurance company offering Systems Safety advice and Reliability, Availability and Maintainability assurance support to a range of industries worldwide. Our web site is located at [www.pmsafety.co.uk](http://www.pmsafety.co.uk)