Removed Appendix B (published papers) pp. 318-336

Maximum Risk Reduction with a Fixed Budget in the railway industry

by

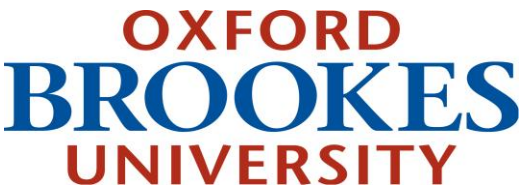
Eberechi Weli

Faculty of Technology, Design & Environment
Oxford Brookes University

A thesis submitted in partial fulfilment of the requirements of Oxford Brookes University for the degree of

Doctor of Philosophy

November 2013



Abstract

Decision-makers in safety-critical industries such as the railways are frequently faced with the complexity of selecting technological, procedural and operational solutions to minimise staff, passengers and third parties' safety risks. In reality, the options for maximising risk reduction are limited by time and budget constraints as well as performance objectives.

Maximising risk reduction is particularly necessary in the times of economic recession where critical services such as those on the UK rail network are not immune to budget cuts. This dilemma is further complicated by statutory frameworks stipulating 'suitable and sufficient' risk assessments and constraints such as 'as low as reasonably practicable'. These significantly influence risk reduction option selection and influence their effective implementation.

This thesis provides extensive research in this area and highlights the limitations of widely applied practices. These practices have limited significance on fundamental engineering principles and become impracticable when a constraint such as a fixed budget is applied – this is the current reality of UK rail network operations and risk management.

This thesis identifies three main areas of weaknesses to achieving the desired objectives with current risk reduction methods as:

- Inaccurate, and unclear problem definition;
- Option evaluation and selection removed from implementation subsequently resulting in misrepresentation of risks and costs;
- Use of concepts and methods that are not based on fundamental engineering principles, not verifiable and with resultant sub-optimal solutions.

Although not solely intended for a single industrial sector, this thesis focuses on guiding the railway risk decision-maker by providing clear categorisation of measures used on railways for risk reduction. This thesis establishes a novel understanding of risk reduction measures' application limitations and respective strengths. This is achieved by applying 'key generic engineering principles' to measures employed for risk reduction. A comprehensive study of their preventive and protective capability in different configurations is presented.

Subsequently, the fundamental understanding of risk reduction measures and their railway applications, the 'cost-of-failure' (CoF), 'risk reduction readiness' (RRR), 'design-operational-procedural-technical' (DOPT) concepts are developed for rational and cost-effective risk reduction.

These concepts are shown to be particularly relevant to cases where blind applications of economic and mathematical theories are misleading and detrimental to engineering risk management.

The case for successfully implementing this framework for maximum risk reduction within a fixed budget is further strengthened by applying, for the first time in railway risk reduction applications, the dynamic programming technique based on practical railway examples.

Key words: **Risk Reduction, Cost Effectiveness, Decision Support, Systems Approach, Organisational Readiness, Budget Constraints, Optimisation, Dynamic Programming.**

Acknowledgements

There's no replacement of God's special grace and for this I'm eternally grateful.

I would like to thank my supervisors, Professor Michael T. Todinov and Professor Khaled Hayatleh for their patience and encouragement. The depth of Michael's knowledge and ability to transfer that knowledge is amazing. A skill I hope to build up and apply successfully someday. Our conversations through this project have traversed risk management, economics, banking, nuclear, transport, environment, family, shipping, oil and gas, mathematics, sports, and politics – name it. During the conversations, we always found relationships between these topics and the research project and in that time, I learnt so much.

This doctorate could not have been completed without the support and patience of my loving wife, Seyi and daughter, 'Kenum. I am grateful to my mother whose prayers focuses my thoughts and continues to help direct my journey. Thanks to a doting sister, Achi for her patience through the beginnings of this work, Tuts always provided me with me a reason to get ahead, Ada-O.T. for listening and providing sound advice, my departed father and uncles for providing this platform and guidance since childhood.

I would like to thank my colleagues Dr. Josh Ahmed, Dr. Alastair Faulkner and Dr. Ivan Lucic for lending their many years of experience of systems and safety engineering. They have listened attentively to my presentations, and provided challenging questions which have been both provocative and constructive. Finally, thanks also to Frances Kennett for her time during the completion stages of this work.

This work has been supported by DJ Hants Ltd, whose grant made this all possible.

This work is dedicated to my departed grandfather - my friend and mentor……..

'Good things don't come easy, easy things are not always the best!'

Table of Contents

Figures

Tables

Acronyms and Abbreviations

Acronym	Definition
ADP	Approximate Dynamic Programming
AHP	Analytical Hierarchy Process
ALARP	As Low As Reasonably Practicable
ASPR	Annual Safety Performance Reports
ATC	Automatic Train Control
ATOC	Association of Train Operating Companies
ATOC	Automatic Train Operation
ATP	Automatic Train Protection
BTP	British Transport Police
CBA	Cost Benefit Analysis
CBT	Collision Between Trains
CCF	Common Cause Failure
CCTV	Closed Circuit Television
CEA	Cost Effectiveness analysis
CEM	Crash Energy Management
CENELEC	European Committee for Electro-technical Standardization
CFT	Component Fault Trees
CoF	Cost of Failure
CPF	cost per statistical fatality avoided
CRI	Centre for Regulated Industries
CSI	Common Safety Indicators
CST	Common Safety targets
DfT	Department for Transport
DOPT	Design Operational Procedural Technical
DRRO	Design Risk-Reduction Options
DSPN	Deterministic Stochastic Petri Nets
EA	Enforcing Authority
EB	Emergency Braking
ERA	European Rail Agency
ERTMS	European Railway Train Management System
ETCS	European Train Control System
EUT	Expected Utility Theory
FMEA	Failure Modes Effect Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FPTC	Failure Propagation and Transformation Calculus
FPTN	Failure Propagation and Transformation Notation
FRAM	Functional Resonance Accident Models
FTA	Fault Tree Analysis
FWI	Fatalities and Weighted Injuries
GAME/ GAMAB	Globalement au moins equivalent (Globally at least equivalent)
HC	House of Commons
HEART	Human Error Assessment and Reduction Technique
HFACS	Human Factors Analysis and Classification System
Hip-HOPS	Hierarchically Performed Hazard Origin and Propagation Studies

HLOS	High Level Output Specification
HMRI	Her Majesty's Railway Inspectorate
HRA	Human Risk/Reliability Assessment
HS	High Speed
HSE	Health and Safety Executive
HSG	Health and Safety Guide
HSL	Health and Safety Laboratory
HSW	Health and Safety at Work
ICP	Independent Competent Person
IEA	Institute of Economic Affairs
IEC	International Electro-technical Commission
IM	Infrastructure managers
INFRACO	Infrastructure Companies
JNP	Jubilee, Northern and Piccadilly
LU-QRA	London Underground Quantitative Risk Assessments
MEM	Minimum Endogenous Mortality
MOU	Memorandum of Understanding
NERA	National Economic Research Associates
NET	Nottingham Tram
NR	Network Rail
NRV	National Reference Values
OPO-CCTV	One-Person-Operated Closed Circuit Television CCTV
ORR	Office of Railway Regulation
ORRO	Operational Risk-Reduction Options
PED	Platform Edge Door
PESP	Platform Emergency Stop Plungers
PIM	Precursor Indicator Model
PPP	Public Private Partnership
PRRO	Procedural Risk-Reduction Options
PSI	Passenger Safety Indicator
PTI	Platform Train Interface/Incidents
QRA	Quantitative Risk Assessment
R2P2	Reducing Risk Protecting People
R3M	Risk Reduction Readiness Model
RA	Railways Act
RIAM	Risk Informed Asset Management
RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
ROGS	Railways and other Guided Transport Systems
RSC	Railway Safety Case
RSD	Railway Safety Directive
RSSB	Rail Safety and Standards Board
RTD	Ready to depart
SCAT	Speed Control After Tripping
SDO	Selective Door Operation
SEFT	State-Event Fault Trees
SFAIRP	So Far As Is Reasonably Practicable
SFT	stress free temperature

SH&E	Safety Health and Environmental
SMIS	Safety Management Information System
SMS	Safety Management System
SPAD	Signals Passed at Danger
SRA	Strategic Railway Authority
SRM	Safety Risk Model
SSP	Strategic Safety Plan
TAG	Transport Analysis Guidance
THERP	Technique for Human Error Rate Prediction
THR	Tolerable Hazard Rates
TMA	Train Movements Authority
TOC	Train Operating Companies
TOR	Tolerability of Risk
TPWS	Train Protection and Warning System
TRACEr	Technique for Retrospective Analysis of Cognitive Errors
TRAIL	Transport Availability Infrastructure and Logistics System
TRRO	Technical Risk-Reduction Options
VPF	Value of Preventing a Fatality
WSF	Wrong-side failures
WSP	Wheel-slip/Wheel-slide Protection system
WTP	Willingness to Pay
1oo2	1 out of 2
1oo1	1 out of 1
2oo2	2 out of 2
2oo3	2 out of 3

Chapter 1 Introduction

Risk management, in general, has evolved through publications, guidelines and standardising practices. On the UK railways, the management of safety risks has in the past two decades, evolved significantly, primarily driven by fatal accidents. To date, this evolution has not been properly critically evaluated. The critical evaluation is required to determine the validity and practicality of the current framework for risk management, employed for delivering the overall risk management objectives in the face of growing concern about the state of the railways and its management.

The existing and on-going 'spending cuts' has negatively affected the investments in infrastructure and rail renewal projects in the UK amidst increasing regulatory and performance requirements, increasing passenger numbers and the increasing need for improved passenger safety. Furthermore, the adoption of rigorous European regulations into UK rail transport introduces the practical obligation to achieve a maximum risk reduction within available funds.

The key safety regulations, which are mandatory, can only be achieved by introducing and implementing techniques that further reduce or eliminate the level of uncertainty inherent in existing risk management practices. The decision-maker is frequently faced with decisions on the selection of options for risk reduction within the available funds. The goal being to ensure risk reduction is optimised to ALARP (As Low As Reasonably Practicable) levels within budget constraints.

The most widely accepted and practiced method by regulators, operators and contractors to achieve the goal of maximum risk reduction within available budgets is the use of Cost-Benefit techniques to select options for optimising risk reduction. The criticisms and present-day awareness of the inaccuracies and uncertainty of the CBA method are well documented and presented. To reduce the inaccuracies, there is a heavy reliance on sensitivity analysis methods. This thesis also shows that for safety risk management decisions, sensitivity analyses are incorrectly used to address the challenges with the method. The increasing reliance on sensitivity analyses is demonstrated by the significant effort that has been directed towards developing sensitivity analysis methods which themselves are flawed, in most cases unverifiable and lack the engineering basis for making robust arguments within operational safety cases. In addition, the case studies based on real examples further demonstrate that cost-benefit methods just do not deliver optimal results once budget constraints are introduced – budget constraints are today's reality.

The techniques used for risk reduction given options flag the absence of systematically and comprehensively justifiable methods for optimising risk reduction given budget constraints. The failure to introduce robust practicable techniques to optimise risk reduction when faced with budget limitations leads to inaccurate assessment of options for risk reduction and potentially wide reaching adverse

effects. A number of examples where these failures are catastrophic are evaluated and presented in this thesis.

This thesis and supporting published work are supported by extensive research on existing techniques for optimum risk reduction within budget constraints. The thesis starts by outlining examples of the current practice. By considering these practices with inherent deficiencies, the thesis develops an accurate definition of the problem and subsequently reviews, in detail, applications and limitations of the use of the CBA (Cost Benefit Analysis) technique.

The aim of this work as part of a PhD research programme is to develop a novel solution for the problem of optimising risk reduction within a fixed budget which is systematic, verifiable and looks to:

- Support the decision-maker or risk analyst by providing a comprehensive framework (with concepts, methods and tool) that will facilitate decision making on risk reduction
- Satisfy regulatory requirements whilst introducing a commercially viable risk management framework;
- Enhance the safety of rail industry staff, passengers and others;
- Minimise losses (such as cost) that is currently almost uncontrollable on railway projects

To illustrate the scale of the current need to develop a framework that addresses the issue of maximising risk reduction given a fixed budget, Tube Lines (the only remaining Infraco of the three initial Infraco companies responsible for renewal works and maintaining the London Underground) had recently received the Public Private Partnership (PPP) Arbiter's final decision on the scope and cost of work it must deliver over the second review period of the PPP Contract (from mid-2010 to 2017) which it has with London Underground Limited following a long standing dispute on cost of projects. The arbiter announced an increase in the final settlement from approximately £4.4 to £4.5 billion from Tube Lines initial formal submission of £6.8 billion. This means that Tube Lines will, in a bid to deliver uncompromised services to the railway public, work within tight budgets, approximately 34% less than Tube Lines had initially proposed. The research is particularly important as it looks to save costs whilst not just maintaining but enhancing safety.

The general approach adopted in the thesis is presented in three phases, to highlight the solution to the problems facing the railway industry.

- Phase 1 – Evaluation of railway network safety risks, regulations, costs and risk evaluation and management practices with strengths and limitations (Chapters 2, 3 and 4)

- Phase 2 – Reviews (literature and practice) and introduction of structured concepts and applications for achieving this goal (Chapters 5, 6 and 7)
    - Cost of Failure concept
    - Principles of Risk Reduction
    - Functional Capability of Risk Reduction Options
    - Dynamic Programming in risk reduction
    - Readiness for Risk Reduction
    - Design Operational Procedural and Technical (DOPT)
    - Amount of risk removed by a Risk Reduction Option
- Phase 3 – Examples of application of the solution, outcomes and conclusions; contributions and recommendations for future work (refer to Chapters 8 and 9).

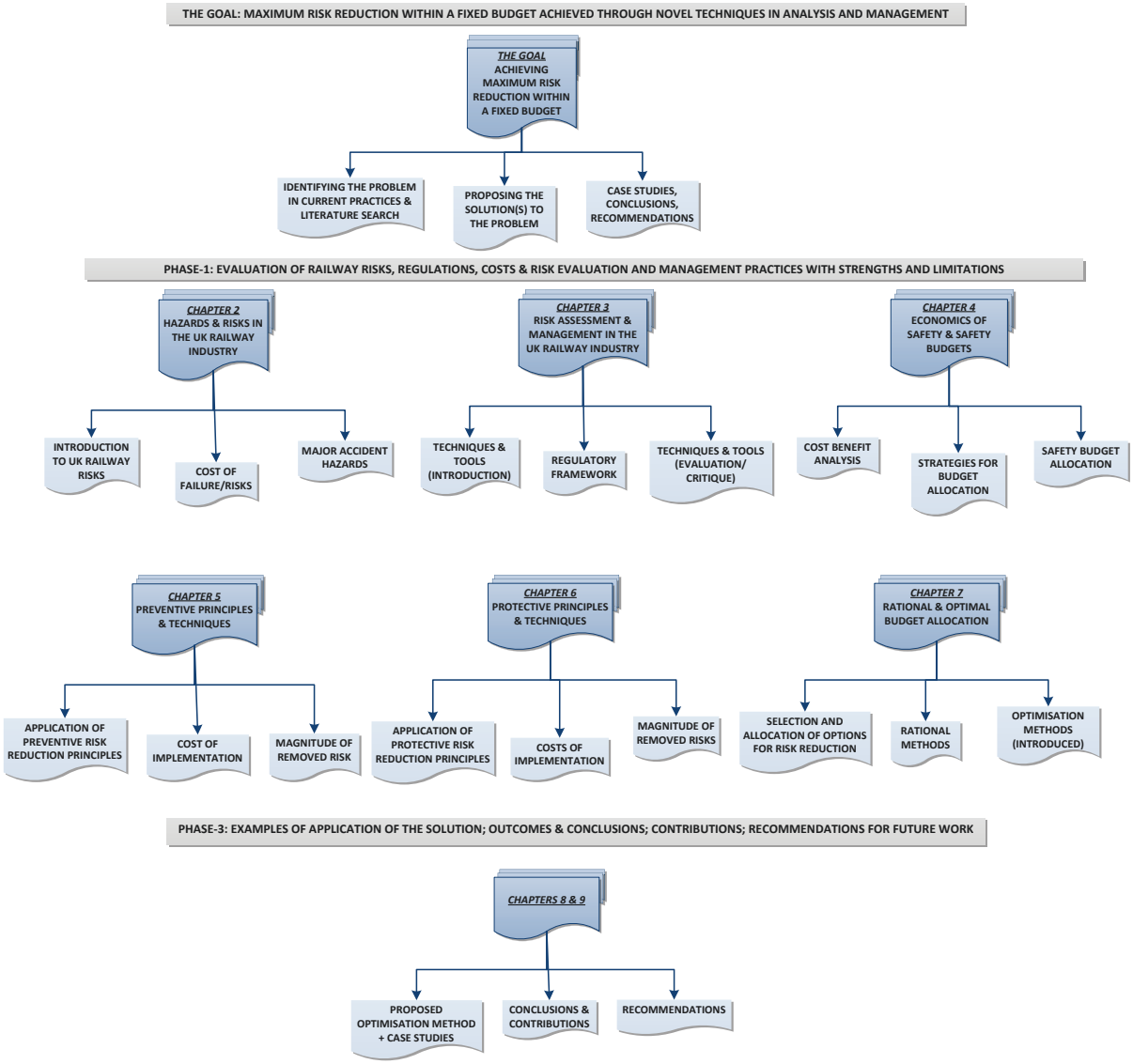


Figure 1: Structure of the thesis

Chapter 2 examines the impact of railway safety and the legal framework for the current risk management practices. This chapter presents the regulatory basis for risk reduction that directly applies to operating the UK railways, introduction to the safety performance of the railways in the last two decades and highlights the 'tipping point' for railway safety i.e. railway privatisation. This chapter also illustrates, using railway operations and performance data, the link between investments, passenger growth and safety performance (by reviewing over ten years safety performance data) on mainline and other railway networks in the UK. The scene is then set for a critical evaluation of the key factors that have affected and will continuously impact decisions made on the safety of the railways. To help achieve the objectives of this chapter, an in depth study of the major railway accidents which resulted in the rapid evolution of the UK railway has been undertaken and presented.

Chapter 3 introduces the currently practiced risk assessment and management techniques, provides a thorough review of these techniques, including benefits and disadvantages. Chapter 3 also comprehensively outlines the application of these techniques within the current regulatory framework and their cost implications. This naturally leads to discussions and a thorough review of the concepts of ALARP and TOR (Tolerability of Risk) presenting practical examples of how decisions are reached using current decision-making techniques. In this chapter, this thesis considers the feasibility of risk acceptance criteria in the evolving regime of regulations and the impact of accidents on the existing risk assessment and risk management strategy.

Chapter 4 introduces and focuses on the financial challenges and cost implications of Achieving Maximum Risk Reduction and is suitably titled – Economics of safety and safety budgets. This chapter presents the initial platform for an evaluation of the use of the cost-benefit approach, supporting quantitative tools and techniques used for optimum risk reduction selection. In this chapter, a thorough review of CBA and its application to risk reduction is presented. In addition, an exhaustive review of Expected Utility Theory in its application as an alternative methodology in optimising risk reduction in safety-critical industries (primarily engineering applications) is also presented.

With the inadequacies in current practice established by the conclusive research and study of railway accidents and extensive review of railway industry norms in the preceding chapters, Chapter 5 and 6 comprehensively present the basic principles and application of risk reduction within the railway network. These chapters present in-depth study on the essential link between the risk reduction principles and their preventive and protective applications. This review of risk reduction options and how they are currently used in the railway industry is systematic and considerably simplifies the work of risk analysts.

By using practical examples, preventive and protective options are subsequently presented with examples of best application. Most importantly, these chapters provide the risk analyst with a comprehensive method of identifying the limitations or strengths (i.e. functional capability) of each option or combination of options in specific applications. This knowledge is further structured and enhanced by the provision of a method for classifying options in their best use as protective, preventive or dual. The concept 'Dual' = means that for the particular application, the option can be equally beneficial for reducing the likelihood of the accident as well as for reducing the consequences in the event of an accident. By this novel work we present a verifiable and distinctive classification of measures as preventive, protective or dual for different failure contributors and scenarios.

The classification and tables provided in the appendices for the railway safety risk analyst is an extensive outline for ease of assessments and option selection that support the maximisation of risk reduction within fixed budget. The tables presented address Collision Between Trains, Derailment and Platform Train Interface accidents. Level crossings related accidents are not addressed in this work.

Considering the comprehensive reviews, the practical knowledge of options and their best application cases, Chapter 7 introduces concepts and methods that support the risk evaluation and option selection process. This chapter underlines the deficiencies in the process of risk reduction and offers solutions through concepts and methods such as:

- Risk Reduction Readiness Model
- D-O-P-T (Design Operational Procedural Technical) Assurance
- Amount of risk removed by a risk reduction option

Finally, a conclusive optimisation solution to the existing problem of maximising risk reduction within a fixed budget is presented. Being a novel application of dynamic programming in an area previously and incorrectly dominated by the cost-benefit method, several test cases and validation tests are undertaken and provided in so doing reinforcing the case for the superiority of the optimisation method proposed.

Chapter 2 Hazards and Risks in the UK Railway Industry

Chapter 2 presents the key railway regulations and regulatory framework that support railway safety. Railway accidents, inquiries and actions such as the privatisation of the railways, amendments to railway operational management are also presented. Furthermore, this chapter looks at the costs of the railway accidents, effect of privatisation on safety and associated costs of failures prior to and following major modifications to the railways. The lessons learned from the major accidents, a significantly important aspect of risk management is evaluated, providing the basis for the concepts and methods introduced for optimising risk reduction in later sections of this thesis. These lessons from the major inquiries into the railway accidents resulted in proposals for enhancing safety management through improvements in:

- Leadership
- Performance criteria and monitoring
- Alignment of the UK railway industry with the European Railway Train Management System/European Train Control System (ERTMS/ETCS)

2.1 Overview of UK Railway Safety

The discussion of railway safety is best addressed by an initial presentation of key changes in the enforcement of UK railway safety regulations and further evaluation of the railway safety decision-making process.

The major changes in the current enforcement of health and safety policy on UK railways are a significant consequence of the 2004 railway review. It proposed primary reforms, including the abolition of the Strategic Railway Authority (SRA), its replacement by a group within the Department for Transport (DfT), and the transfer of safety regulation to the Office of Railway Regulation (ORR).

Before 2006, health and safety policy and enforcement on UK railways was the responsibility of the Health and Safety Executive (HSE). This responsibility was duly handed over to the Office of Railway Regulation (ORR) and the transfer currently means that the ORR oversees the regulation of the operation of the railways and other guided transport systems including heritage, metros and light rail systems. The Railways and Other Guided Transport Systems (Safety) Regulations provide the regulatory regime for rail safety within the UK. Railways and Other Guided Transport Systems (Miscellaneous Amendments) Regulations 2013 came into force on the 21st May 2013.

The basis of this transfer is set out in a Memorandum of Understanding (MOU) between the Health and Safety Executive (HSE) and ORR. The purpose of the MOU is to ensure the effective coordination and cooperation between these organisations in relation to the regulation of health and safety, including policy matters and the enforcement of health and safety law on railways, tramways and other guided

transport systems in Great Britain. Some of the most important guiding statements are that the HSE considers the MOU as a facilitator of the performance of its functions, in accordance with the Health and Safety at Work Act from 1974. For its part, the ORR acknowledges that the MOU, in accordance with the Railways Act 2005, contributes to the provision of appropriate arrangements for fulfilling its duties in relation to the railway safety purposes. In addition, the MOU ensures that the allocation of responsibilities set out in the Health and Safety (Enforcing Authority for Railways and Other Guided Transport Systems) Regulations 2006 works effectively and provides clarification for duty holders as required. The Health and Safety (Enforcing Authority for Railways and Other Guided Transport Systems) Regulations allocates enforcement functions to ORR and defines who the Enforcing Authority (EA) is for particular activities and in relation to certain premises.

Another significant step towards enforcing health and safety regulatory policy is that the Railway Act 2005, also as a result of the 2004 railway review, places a statutory duty on the government to set out every five years:

- How much public expenditure it wishes to devote to rail;
- What the railway is expected to deliver in the key areas of safety, reliability and capacity.

The UK government presents a five-yearly strategy on the delivery of a sustainable, modern railway by the publication of white papers on proposed plans for improving safety and performance to the public.

In order to fully investigate the overall performance of the UK Railway system over time (past two decades), a review was undertaken of considerable research in the areas of customer behaviour, justifying investments in railway safety and reliability. Some of the research has been independent, but most of it was instigated by the government through the Health and Safety Executive (HSE), the Office of Railway Regulations (ORR), the Department for Transport (DfT) and the Railway Safety and Standards Board (RSSB). These noteworthy publications, usually annual, provide comprehensive information on the current state of the railway and details of the methodology to safety planning in the industry. These are based on duty holders' initiatives and the projections of the safety benefits they aim to achieve. These sources are:

- 'Transport Statistics Bulletins' produced by the Department for Transport
- 'Annual Safety Performance Reports' published by the Railway Safety and Standards Board
- 'The Railway Strategic Safety Plans'
- The HSE's 'Annual Reports on Railway Safety'

These reports are principally sources of statistical data derived from the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995, including information on key findings and trends. RIDDOR refers to the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations that provide a set of health and safety regulations. RIDDOR mandates the reporting of work-related accidents. The Railway Strategic Safety Plans, RSSB (2008), RSSB (2007) were developed by the rail industry in consultation with the DfT, ORR, SRA, HSE, Trade Unions and Rail Passenger Council, in order to analyse the current railway risk profile, identify priorities, comprehensively outline the steps to resolve the priorities, and demonstrate the industry's commitment to safety as the foundation of an efficient, well-run railway.

The primary industry source for information on the safety performance of the mainline railway is the Annual Safety Performance Reports (ASPR) produced by the RSSB, which provides safety intelligence and risk information to RSSB members, rail employees, passengers, the government and its agencies and the public at large. These reports are annual for consistency with its associated High Level Output Specification (HLOS) and the Railway Strategic Safety Plan (SSP). They contain reviews of performance levels across a number of topic areas and consider how key safety issues are addressed by the industry (RSSB 2010). The areas addressed include those identified in the Railway Strategic Safety Plan (SSP) which covers a five year period.

The ASPR's scope is generally limited to incidents that occur in stations, on trains, or elsewhere on the mainline railway infrastructure such as the track and the trackside. Workforce fatalities that occur away from these locations, but during working time, are also included, although not used as part of this work.

Most analyses in the ASPR are based on data from the Safety Management Information System (SMIS). However, this is supplemented where appropriate with data from other sources, such as British Transport Police (BTP), the Office of Rail Regulation (ORR) and Network Rail. Where a chart or table has been derived from a source other than SMIS, it is referenced. Thus the Safety Risk Model (SRM) is updated regularly, and it is from this model that the key risk areas are determined. Changes in the level of risk and hence progress against the trajectories are reviewed and updated as the risk models are updated. Performance is fundamentally monitored by individual duty holders and their own systems, but also at the national level using SMIS, the SRM, and through the production of periodic and special topic reports. As a result of this monitoring, corrective actions may be initiated by individual companies, or collectively through new or revised national programmes, standards changes etc. The regular review of performance at the national level is overseen by the RSSB through a series of papers considered as part of the 'Strategic Board Agenda'. Individual, national, cooperative groups monitor performance in particular areas and agree collective actions where appropriate. The report includes comprehensive statistical

analyses on a wide range of safety performance indicators: many concern the actual safety performance level that has been achieved; others provide a measure of the underlying risks.

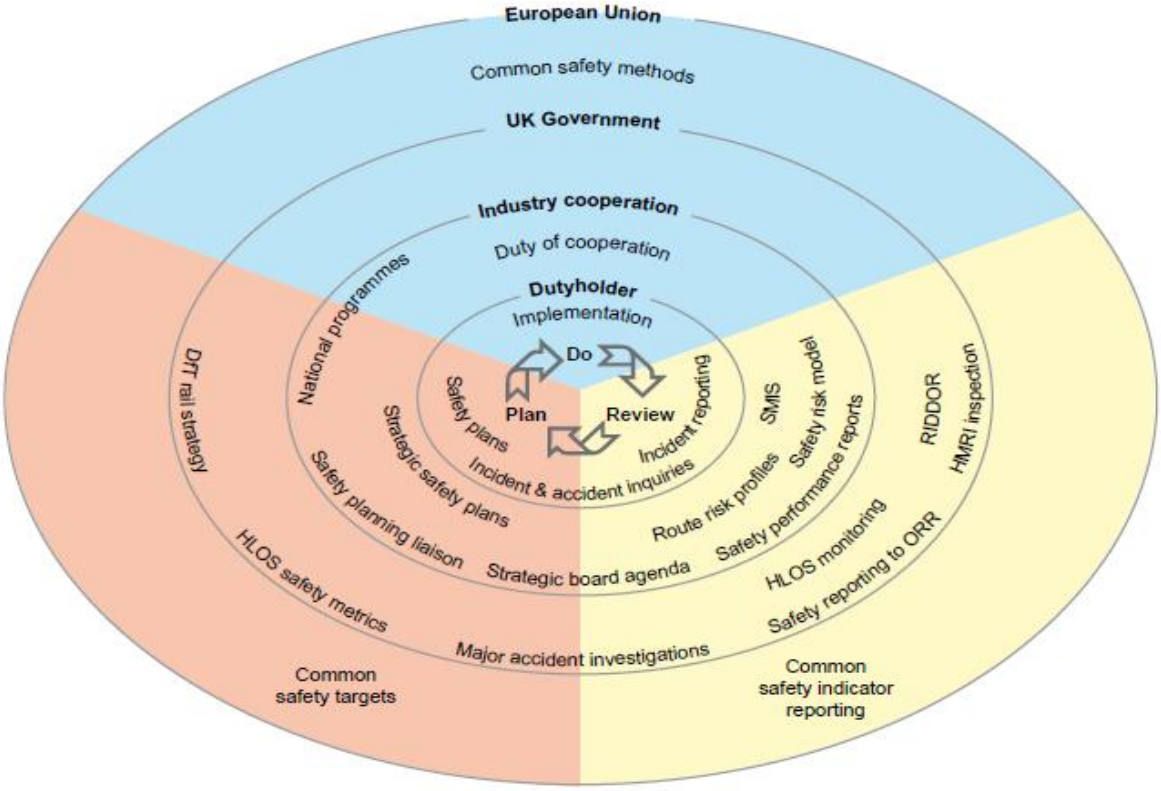


Figure 2: Railway Industry Safety Planning Lifecycle (Railway Strategic Safety Plan 2008-2010)

Figure 2 illustrates the industry's planning cycle, based on a plan-do-review model. The Strategic Safety Plan (SSP) fits into the 'plan' sector of the model, at the industry cooperation level, bringing together the planning work done by duty holders and taking into account the input from the UK Government and the European Community. Implementation is primarily a duty holder responsibility, although some activities are coordinated by RSSB as National Programmes.

A critical review of these separate publications over a ten year period, with the aim of linking their objectives, demonstrates a convergence of intended functions to the key challenges faced by the railway industry. These can be summarised as:

1. Predicting future safety performance and maintaining a pre-determined level of safety.
2. Reducing the cost of delivering a safe railway.
3. Developing and maintaining competency across all personnel levels on the railway.
4. Safety assurance for the infrastructure, rail vehicles and associated systems.

The reports also provide a mechanism for disseminating information about the work of Her Majesty's Railway Inspectorate (HMRI) and an opportunity to cascade messages on emerging issues and findings from these investigations which would not necessarily justify separate publications.

In response to notable accidents such as the Hatfield train accident, the three railway accident statistical papers by Evans (2003, 2005, 2007) are prominent sources supporting the view that improvements have been made following the 2004 railway restructuring.

The results of interviews with key people in the railway industry, together with a review of submissions from key interested parties are outlined in the Centre for Regulated Industries paper, CRI (2005). The findings were that all major characteristics of the rail reform in Britain were seen as workable, while empirical data revealed that as a result of the reforms prior to the Hatfield train crash, improvements had been comparatively successful. However, some failings were noted, such as in the introduction of a private infrastructure manager. This was due to indecision over refranchising and partly the after-effect of the Hatfield crash. This undoubtedly affected general passenger perception of railway safety, leading to the general view that the 1994/95 privatisation, the 2004 railway review, and other implementations that followed have actually worsened the railway performance.

2.2 Railway Privatisation and Safety

The analysis of railway accidents between 1967 and 2010, by different railway accident research groups and government organisations clearly indicate that the privatisation of the railways did not degrade safety performance, despite a stream of opponents to the statistical evidence made available by Evans (2007), and DfT (2010).

Following the privatisation of British Rail in 1994/95, the number of journeys increased by 71% from 735 million to 1,258 million between 1994/95 and 2009/10. 35% of this increase was realised since 1999/2000 (DfT, 2010). Within this period, the recorded high fatality rates resulted from major accidents such as at Ladbroke Grove in 1999. However, the transport accident statistics show that only one passenger fatality has occurred since 2005. A major accident is a single incident with high consequences. Most cases of fatality or major accidents since 2005 have been as a result of train movements (TMA). These led to injuries and fatalities as a result of train movement, whilst the train itself is not involved in the accident (these have been discussed in Section 2.3 of this thesis).

Examples of TMA include people falling from moving trains; when passengers alight from a moving train; or getting caught between carriage doors as a train moves away from the platform. In Chapter 8, a railway case study (Passenger Door Trap and Drag) of this type of major accident is used to illustrate the

benefit of applying the proposed maximum risk reduction methodology. In 2008, TMA resulted in 18 fatalities, but was reduced by half in 2009.

A further indication of safety failures used in overall safety performance evaluation is Signals Passed at Danger (SPAD). Records for the period 2002 - 2009 show a gradual fall in reported incidents from 382 to 261. DfT (2010) states that the number of cases where a SPAD could have led to a potentially severe accident in that same period fell by over 80% while non-significant cases increased by 16%. Thus the number of severe cases dropped from 58% to 29% for all reported SPAD incidents.

Despite these readily available empirical data and accident analysis reports, there is still a fast growing number of people claiming that the privatisation of the railway has resulted in the degradation of safety and non-conformance to regulatory policy. Leading the rapidly increasing publications of the negative views are Wolmar (1996, 2001, 2005), Nash (2002), and Glaister (2002). The public perception of the state of the railways after privatisation was matched by widely publicised arguments from transport economists and historians finding the culprit in the governmental policy. The government's inadequacy in setting appropriate standards for the industry and lack of delivery of value for the invested capital were highlighted further after the Hatfield crash. Critics identified cost *escalation (i.e. the excessive spending) on safety as a consequence of:*

- *the absence or lack of a structured decision making process;*
- *the poor service quality;*
- *the deficiencies in the reconciliation of different stakeholders' aspirations in the efficient planning of services and investment*.

The disparity in views from the public and opponents of railway privatisation, compared with the empirical analysis and other data mentioned above raises vital questions on the *mismatch between the perception and the reality of current state of rail safety*.

Suggestions made by Evans (2007) that reports of images of fatal rail accidents at Southall, Ladbroke Grove, Hatfield and Potters Bar all figure prominently in the public perception of rail safety is supported by the Institute of Economic Affairs, IEA (2006). The IEA publication on the relationship between the railways, government and market structure provides simple clues to these precise issues: government interference, decision-making problems, in conjunction with the high expectation from passengers who are paying for these services. At privatisation, the government imposed a structure upon the industry that might never have evolved if the market had been left without interference. The splitting apart of the provision of track stations and signals from that of the rolling stock and the running of trains was a decision taken by government ministers, not business people. The authors of the IEA report suggested

that the privatisation approach taken was akin to government officials walking into a hotel and demanding that it be owned by one company, the reception and reservations run by another and the beds leased from a third. The report argues that the division of responsibilities might be appropriate in the railway industry, but queried whether the government should make these decisions. As Newman (2003) pointed out, 'the power of stories over statistics' is fundamental to the belief that safety deteriorated after privatisation. Accounts of railway accidents make exceptionally compelling and tragic reading and are easier to comprehend than a chart presented before the public. Newman notes that accounts of accidents are particularly persuasive when they come from those who were directly involved; these include not only the bereaved and injured, but railway staff, rescue workers, and other witnesses.

In addition, the British people have always been rather sentimental and emotional about the railways. This might be one reason why railways have mistakenly been treated and regulated as monopolies from the early days. Further arguments demonstrate that the basic structure of the industry at privatisation was a workable way of introducing competition, but was marred by mistakes in implementation. Conclusions from the IEA report suggest that the restructuring and privatisation of British Rail were not as bad as the direst commentators claim:

- Safety performance improved.
- The passenger numbers and services increased.
- The passenger increase resulted in a build-up of wear on the infrastructure at the same time as maintenance input was reduced.
- The net result was a decline in infrastructure quality and a subsequent decline in both line speed and punctuality;
- Rolling-stock quality improved.
- The most notable failure was the escalating cost of operating the railway, directly affecting cost to passengers. The contractual and market structure that was imposed, introduced new risks and unreasonable incentives leading to some dissipation in railway-specific skills and a major increase in operating costs that was out of proportion to the increase in either the quantity or quality of outputs.

To illustrate the safety improvement achieved pre- and post-privatisation, Evans (2005) presented an analysis (Figures 3 and 4) using accident data between 1967 and 2003. The accidents are shown in the figures below as those that occurred in over 27 years, 1967 to 1993 (i.e. pre-privatisation) and those that occurred from 1993 to 2003, or during 10 years post-privatisation. The significant train accident rate was falling at 4.3% per year between 1971 and 1993/94, but with the exception of 1994/95, all the later annual data points are better than that favourable trend. This demonstrates that the fatal accidents that

have actually occurred since privatisation have been slightly fewer than those expected on the basis of the favourable trend established pre-privatisation. Thus there is no evidence that the post-privatisation performance is worse than British Rail might have been expected to achieve.

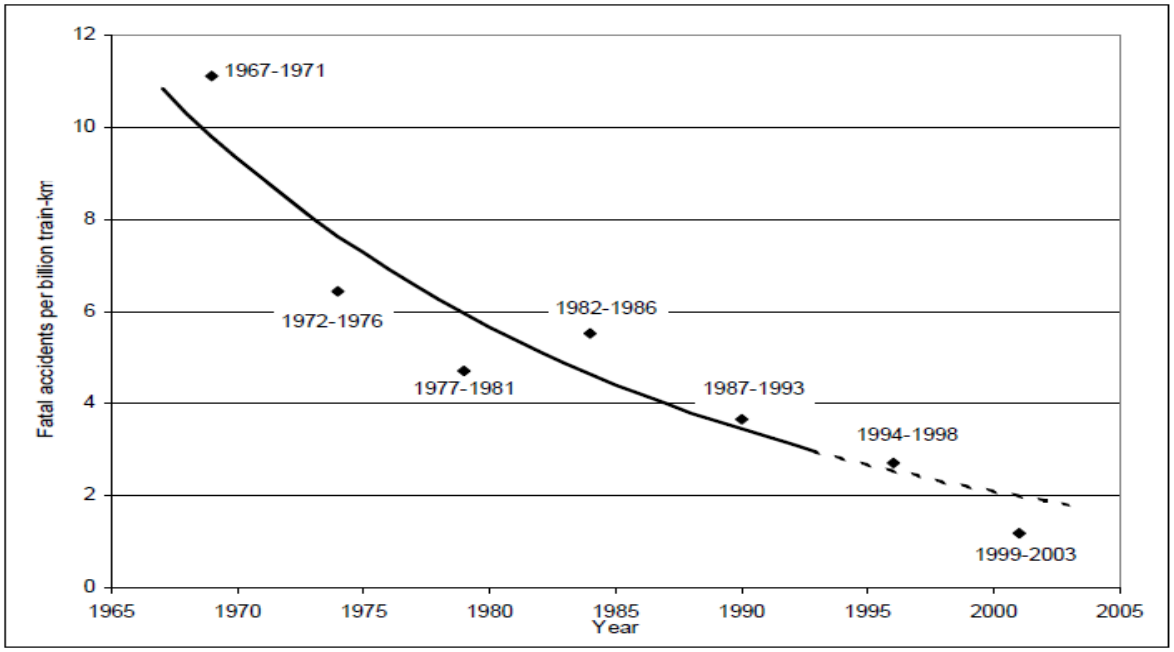


Figure 3: Fatal Train Accidents 1967 – 2003: Great Britain National Rail System. Extracted from Evans (2005)

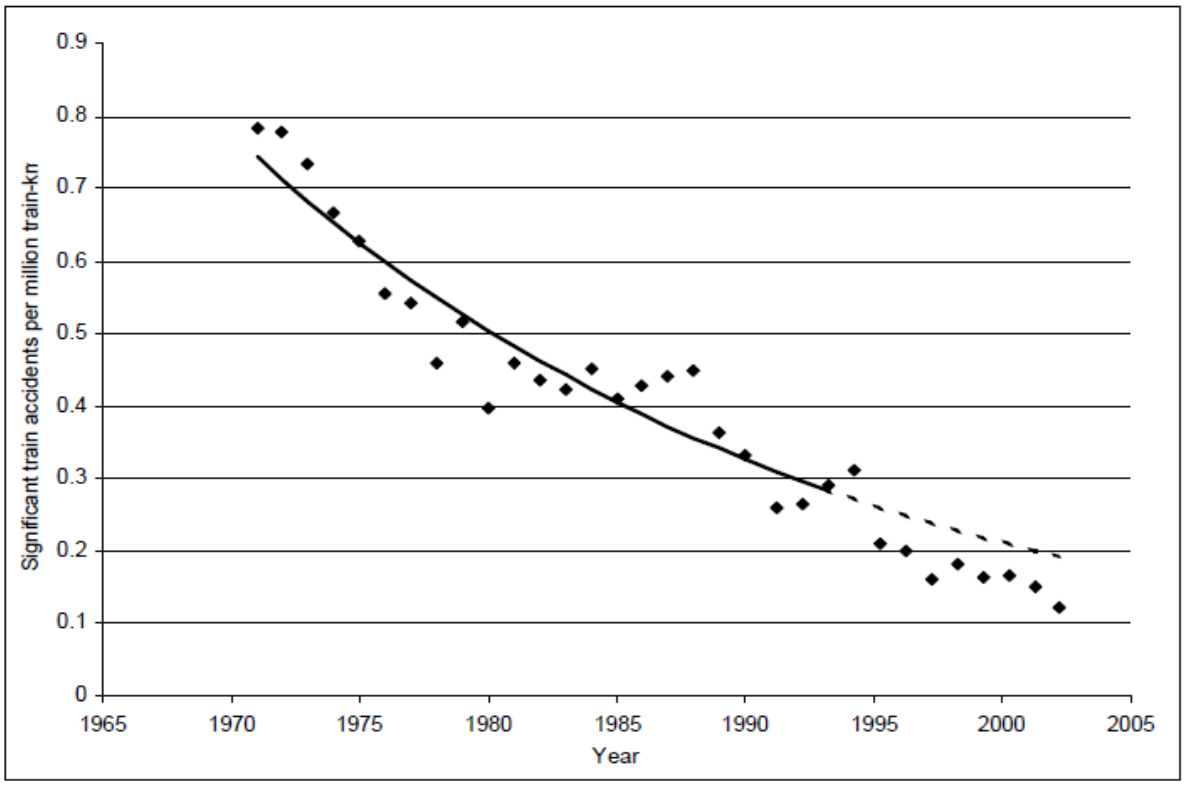


Figure 4: Significant Train Accidents 1971 – 2002/03: Great Britain. Extracted from Evans (2005)

2.3 Hazards and Risks in the Railway Industry

This section introduces the hazards used to analyse the current state of the railways and provides a detailed insight into how the hazards are analysed and reported using the ASPR.

There are some marked differences between the ways hazards are categorised for the different rail transport operators in the UK. Analysis of overall risk profiles for the mainline railways is undertaken by the Railway Safety and Standards Board (RSSB), published in their Risk Profile Bulletins and subsequently in the annual safety performance reports. These two sets of data summarise total risk according to accident categories based on the railway Safety Risk Model (SRM). The SRM analyses 120 hazardous events grouped under the four top events or major hazards: Train Accidents, Train Movement Accidents, Non-movement Accidents and Trespass, while London Underground Quantitative Risk Assessments (LU QRA) focuses on a list of 20 contributors to safety risk. These contributors called 'Top Events' derived from the LU QRA are defined in Table 1 below:

Table 1: Major Hazards - Risk Models

Accident Grouping (Top Event)	Definition
Collision Between Trains (addressed by Train accidents in the SRM)	This is the risk from an incident where there is an impact between two trains. This includes: end on, side on and side swipe collisions between passenger trains on London Underground (LU) and Network Rail (NR) infrastructure; collisions between runaway engineering trains and passenger trains; collisions between derailed/collided trains that initially did not involve a passenger train but there was a subsequent collision with a passenger train
Derailment (addressed by Train accidents in the SRM)	This is the risk from passenger train derailments on LU and NR infrastructure. The description of this risk includes all obstructions on track (including objects fallen from trains) or that infringe the kinematic envelope. It also includes all structural failures (that occur when a train is not present) that could result in the loss of integrity for the track or obstruction on the track.
Collision Hazard (with object)	This is the risk from incidents resulting from an impact between a train and an obstruction (including a fixed or mobile infrastructure). The description of this risk includes collisions with platform edges and terminal platforms, collisions with floodgates and line-side structures (including tunnel walls), but it excludes obstructions on track (which are included in the derailment risk)
Passenger Train Interface (Platform)	This risk of fatality arises from the platform edge where it interfaces with trains and is normally accessible to passengers. The Quantified Risk Assessment (QRA) model also reflects the failure modes that occur if the train moves off without adequate checks, when a person falls from the platform and driver fails to notice a person being trapped in the train doors
Passenger Train Interface (On Train)	This is the risk of fatality related to a passenger who has boarded a train. It includes items within station limits, such as unauthorised use of inter-car doors
Train Fire	This is the risk of fatality involving fire on any part of a train or its contents.
Station Fire	The Station Fire is the risk of fatality associated with fires in both the public and non-public areas of the station; including disused areas and tenancies.

Accident Grouping (Top Event)	Definition
Tunnel Fire	The Tunnel Fire risk of fatality involves fire in sub-surface or tube sections or open sections but not within the confines of the station head and tail walls.
Arcing	The Arcing risk of fatality arises from fire or electric burning from a short circuit or electrical fault on the traction supply, limited only by the resistance of the fault path and protected electrically only by sub-station circuit breakers.
Unauthorised Access (also termed Trespass in the SRM)	This is the risk of fatality arising from unauthorised people being on or around the track, who are not in the vicinity of a station / platform
Loss of Power	This models risk of fatality from any incident associated with major, system wide power loss, which affects, in particular, trains and stations.
Ventilation risk (Subsurface and Tunnel sections)	The risk to customers from being trapped on immobilised trains in sections (i.e. not at platforms) due to all causes except power failure. The conditions within the carriages are assumed to deteriorate by a combination of heat / humidity and the build-up of carbon dioxide. There is also a risk of fatality from self-detrainment (i.e. leaving the train) authorised detrainment without protection

Understanding the classification and definition of these top events is pertinent to undertaking adequate safety analysis and building prediction models based on empirical data. The resulting analyses help the decision-maker select the best options for future investments. These are published in the annual safety reports, easily accessible to the public to demonstrate improvements or failings on the operational railway.

Other risks not identified and defined, such as Escalator Fire, Lift Fire, Explosion, Station Area accident are not considered within this thesis. Some of the defined hazards are only briefly mentioned in later sections of the thesis. The focus of this thesis is on top events or risks that have the most significant impact on cost of failure and achieving maximum risk reduction.

Recently, safety improvement programmes on the railway networks identified six priority residual safety risks that should instruct fundamental improvements to operational safety to achieve the maximum risk reduction objectives:

- Reducing risks to customer accidents at the platform train interface
- Reducing risks of derailment
- Reducing the occurrence of signals passed at danger (SPADs)
- Improving the effectiveness and quality of risk assessment models and related processes which form the effectiveness of risk control measures
- Decreasing the risk of injury to employees and contractors working on the track
- Minimising the impacts of stress and workplace violence on staff

The analyses of these hazards are usually undertaken by dedicated safety analysts within risks groups in each railway operator, who ensure that the risk models are frequently reviewed. The operator's in-house data base and the risk models with Top Events are updated to reflect the current state of the railway and to inform decisions promoting changes to the operational railway.

The data used in this section of the thesis to illustrate this process of hazard analysis is largely derived from the annual safety reports. RSSB (2010) provides details on how the safety report is presented. The annual safety reports analyse safety in terms of fatalities, injuries, shock and trauma. Injuries are categorised according to the level of severity such as fatality, major injury and minor injuries. Fatalities, injuries, shock and trauma are combined into a single failure termed Fatalities and Weighted Injuries (FWI). Each injury is categorised by the hazardous event that caused it and the major precursor or contributing event. The ASPR uses the same set of hazardous events and precursors as the RSSB SRM. The precursors allow risk and performance to be analysed in a number of different ways, for example by focussing on the type or cause of event, or the person type to whom it occurs , whether passenger, workforce or public.

Table 2: Injury degrees and Weightings (Source: RSSB 2010)

Injury Degree	Definition	Ratio
Fatality	Death occurs within one year of the accident	1
Major Injury	Injuries to passengers, staff or members of the public. This includes losing consciousness, most fractures, major dislocations and loss of sight (temporary or permanent) and other injuries that result in hospital attendance for more than 24 hours	10
RIDDOR – reportable minor injury	A physical injury to a passenger, staff or member of the public that is neither a fatality nor a major injury. Minor injuries to the workforce are RIDDOR reportable if the injured person is incapacitated for work for more than three consecutive days. Minor injuries to the passengers and public are RIDDOR-reportable if the injured person was taken from the accident site to the hospital	200
Non-RIDDOR-reportable minor injury	All other physical injuries	1000
Class 1 shock/trauma	Caused by witnessing a fatality or being involved in a collision, derailment or train fire	200
Class 2 shock/trauma	Other causes such as verbal abuse and near misses	1000

Analysis of trends in incident data is provided for each topic. This usually covers at least ten years of available consistently classified data. The safety analyst differentiates between real changes in underlying safety and statistical fluctuations that can occur from one year to the next. For example, annual numbers of passenger fatalities can vary greatly, depending on the occurrence (or not) of low-frequency, high-consequence events, such as train accidents.

However, a year without a train accident does not necessarily indicate improvement in passenger safety, and a year with such an accident does not necessarily imply deterioration. To address this, longer-term trends can be assessed using moving averages, for example over five or ten years. Further understanding of changes in the underlying system risk is gained by looking at trends in accident precursors or 'near misses'.

Statistical significance testing is used to explain whether a genuine change has occurred or whether the data could be the result of random fluctuations. Where statistical testing has been used, the term 'significant' refers to a change that is significant at the 95% confidence level.

Poor data quality is undoubtedly the primary concern of most analysts. In safety analysis, this is at the top of requirements for a near-precise prediction or current state model that reflects the real world, as much as possible. The majority of the analysis is based on data from the industry's Safety Management Information System (SMIS). Their models often do not depend on data quality nor do models apply techniques such as Monte Carlo simulation to expose the range of possible sensitivities and uncertainties. Data quality is a recurring theme in this thesis and rightfully so. In a quest to ensure that the data quality is continuously improved and that the RSSB is currently leading a data quality project, backed by the SMIS Programme Board and Association of Train Operating Companies (ATOC) Operations Council. The SMIS analysts use RIDDOR 95 as the legislative guide that helps determine the scope of events that are to be recorded. In addition, non-RIDDOR reportable incidents and accidents as defined in Table 2 are recorded. The current scope was widened to collect all physical injuries and cases of shock, non RIDDOR-reportable train accidents and a number of precursor events.

2.4 Cost of Failure in the Railway Industry

As a result of the new structure of the railways where engineering cuts across different levels from government to operator and sub-contractors, the cost of failure to a railway operator may be different from the cost of failure to the supplier or manufacturer of equipment. However, the general cost will include several components such as penalty payments, cost of lost production, cost of lost site access, insurance costs, cost of mobilisation of resources for emergency situations, cost of the loss of business due to low passenger confidence.

According to Todinov (2007) losses from failure are often expressed in monetary units as cost of failure. A classification of losses from engineering failures is presented below:

- Losses of life or damage to health
- Losses associated with damage to the environment and the community infrastructure

- Financial losses including loss of production, loss of capital assets, loss of sales, cost of intervention and repair, compensation payments, penalty payments, legal costs, reduction in benefits, losses due to change of laws, product liability, cost overruns, inflation, capital costs changes, exchange rate changes, etc.
- Loss of reputation including loss of market share, loss of customers, loss of contracts, impact on share value, loss of confidence in the business, etc.

Given the definitions above and the classical relationship between the cost of failure, probability of failure and risk of failure as defined by Henley and Kumamoto (1981) and Vose (2000) presented below:

$$K = p_f C \qquad (2.1)$$

where p_f is the probability of failure, C the cost of failure and K is the risk of failure. Equations 2.1 can be modified and used by the government for risk-based investment decisions, the operator for decision making on which safety systems to introduce into the operational railways to meet operational and safety targets, and sub-contractors for risk-based designs.

The cost of failure in this section will be presented in terms of *injuries and fatalities* for simplicity and to explain data used for current accident analyses. In later sections discussions on the cost of failure are presented in *monetary or financial* terms in order to comprehensively address the decision-making challenges when investing in safety to minimise the occurrence of incidents, which could lead to loss of life, injury or damage to assets.

The risk of death from road accidents is approximately 27 times greater than rail. Comparisons in terms of passenger hours per fatality indicate that the ratios are 16 to 1 against road, 5 to 1 against ferry and 18 to 1 for air travel. This demonstrates that rail travel is the safest mode of travel by any rational comparison method. However, statistics of this sort have been questioned, with claims that such comparisons are empirically unjustified. Evans (2005) noted that society could prevent more fatalities at the same cost by devoting relatively more resources to road safety and less to rail safety. However, Flyvbjerg et al.'s (2002) study of the accuracy of cost estimates in transportation infrastructure planning found that for rail projects, actual costs turned out to be on average 44.7% higher than estimated costs, and for roads 20.4% higher. Evaluation of publications on the cost of failure and its corresponding link to investment in transportation shows that a thorough study is yet to be undertaken. It is not surprising that decision making for investment in rail has not been definitive and productive as the public would expect.

The results of extensive research into operator revenues, cost of safety investments and cost directly related to the failure of systems leading to fatalities or injuries are presented in Tables 3 and 4.

Table 3: Rail Systems Passenger Hours (Source: Transport Statistics Bulletin 2008; DfT2008)

	Rail		Underground				London trams			
	National Rail Network		London Underground		Glasgow Subway		DLR (Docklands Light Railway		Croydon Tramlink	
Period	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)
1997/98	846	3,608	832	1,150	14	11	21	18	_	_
1998/99	892	3,854	866	1,218	15	12	28	25	_	_
1999/00	931	4,119	927	1,294	15	12	31	27	_	_
2000/01	957	4,115	970	1,361	14	13	38	35	15	15
2001/02	960	4,178	953	1,355	14	12	41	38	18	15
2002/03	976	4,183	942	1,299	13	12	46	41	19	17
2003/04	1.012	4,329	948	1,289	13	12	49	42	20	18
2004/05	1.045	4,490	976	1,340	13	12	50	44	22	19
2005/06	1.082	4,750	970	1,383	13	12	54	49	23	20
2006/07	1.151	5,184	1,040	1,569	13	14	64	64	25	17
2007/08	1.232	5,555	1,096	1,525	15	14	67	62	27	17
% change over 10 years	46	54	32	33	3	25	217	246	–	–

Table 4: Rail Systems Passenger Revenue (Source: Transport Statistics Bulletin 2008, DfT2008)

	Metro and tram systems outside London											
	Nexus (Tyne & Wear Metro)		Centro West Midland Metro		Nottingham NET Tram		Altram Manchester Metrolink		Stage-coach Supertram		Blackpool trams	
Period	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)	Passenger journeys (millions)	Passenger revenue (£million at 2007/08 prices)
1997/98	35	28	_	_	_	_	14	18	9	8	5	6
1998/99	34	28	_	_	_	_	13	_	10	8	4	5
1999/00	33	30	5	_	_	_	14	_	11	8	4	5
2000/01	33	29	5	4	_	_	17	22	11	9	4	5
2001/02	33	30	5	5	_	_	18	24	11	9	5	6
2002/03	37	33	5	6	_	_	19	24	12	12	5	5
2003/04	38	35	5	6	0	_	19	23	12	10	4	4
2004/05	37	35	5	6	9	6	20	24	13	12	4	5
2005/06	36	36	5	6	10	8	20	24	13	11	4	5
2006/07	38	36	5	5	10	8	20	23	14	12	3	4
2007/08	40	35	5	5	10	8	20	23	15	11	3	4
% change over 10 years	14	22	–	–	–	–	45	24	61	47	-40	-34

The data presented above represents the different rail systems in the UK with passenger hours and revenue between 1997 and 2008. These dates are significant when analysing improvements and investments, because of the railway reviews in 1994 and subsequent privatisation of the mainline railway in 1996. Other privatisation initiatives soon followed with the Private Public Partnership (PPP) of the London Underground in 2002. The PPP was adopted as the government's preferred solution for investing in the Tube under a 30-year contract with three infrastructure companies (Infracos).

The three Infracos were responsible for the maintenance and renewal of London Underground's (LU) assets - its rolling stock, stations, tracks, tunnels and signals. The Tube network is divided into three Infracos. Tube Lines remains responsible for the Jubilee, Northern and Piccadilly lines (JNP) under the PPP contract, and became a wholly owned subsidiary of Transport for London in 2010. The contract requires that they deliver a certain level of daily asset performance, and that they upgrade the assets to deliver improved capability in the longer term. They are subject to financial incentives or penalties based on their delivery against the performance levels set out in the contract.

The data is also affected by important dates such as the Tyne and Wear Metro Sunderland extension opening in March 2002, the West Midlands Metro (Centro) opened in 1999 and Nottingham Tram (NET) opened in March 2004. 20 stations were also transferred from the national rail network to the Altram Manchester Metrolink.

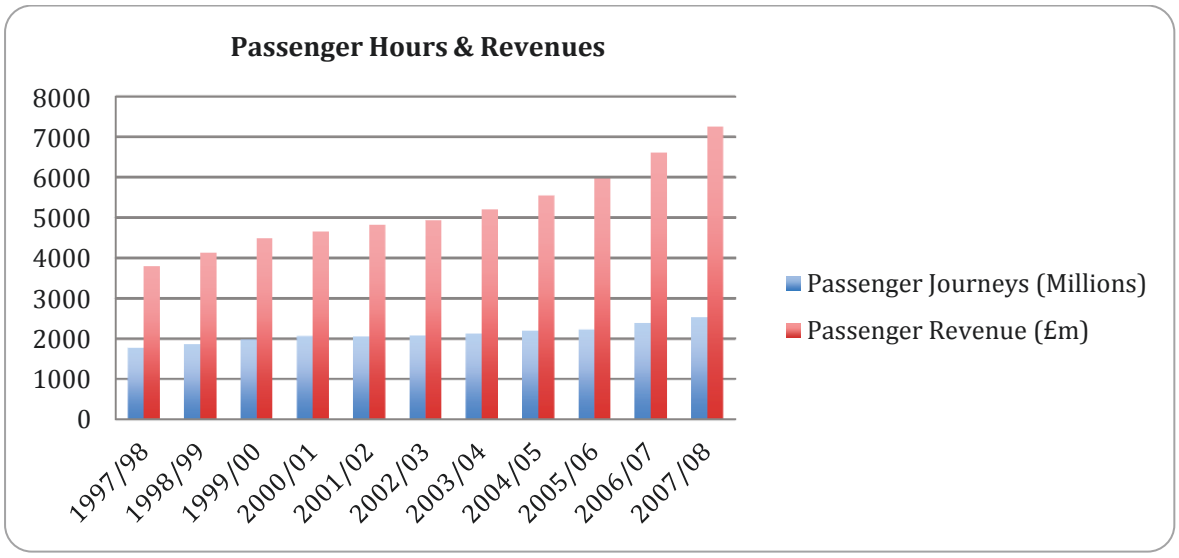


Figure 5: Passenger Hours and Revenue – UK Railway Systems

The data collated gives a total of 1,776 million passenger journeys in 1997/98 and 2,529 million passenger journeys in 2007/2008 indicating approximately 30% increase in the use of the railways over the 10 year period. The UK rail industry also saw a corresponding growth in revenue as a result of the 30% increase in passenger journeys from £3,789 million to £7,251 million over the same 10 year period – a 48% increase.

The question that follows is – has the industry invested in line with this growth to improve safety? According to the results given above, the logical answer to the question will be yes, considering the growth in usage of the railways. One must now consider the safety and investments recorded over the 10 year period.

These tables give the number of train accidents and casualties on all railway undertakings in Great Britain. Railway undertakings are required to report accidents, failures and dangerous occurrences to the Secretary of State for Transport, under the regulatory safety legislation. Beside the data for Network Rail and London Transport railways, the tables also cover accidents on Eurotunnel, tram systems and minor railways.

Table 5: Investment in Rail Transport (Source: DfT 2008)

Period	Rail Infrastructure (£m)		Rolling Stock/Trains (£m)	
	National Rail	Other Rail Networks	National Rail	Other Rail Networks
1995/96	900	1,101	200	121
1996/97	1,178	1,047	47	148
1997/98	1,430	898	114	82
1998/99	1,823	821	176	85
1999/00	2,012	1,1623	236	84
2000/01	2,404	386	554	75
2001/02	3,148	504	922	75
2002/03	3,756	485	566	75
2003/04	4,722	464	774	177
2004/05	3,543	729	897	165
2005/06	3,237	1,219	557	166

Table 5 shows the investment made on the rail transport industry covering rail systems infrastructure and rolling stock between 1995/96 and 2005/2006. There is a demonstrable increase in the government-led investment on the railways with the aim of improving performance and safety as outlined in the Railways Act 2005 (RA 2005). The chart below shows the 55% growth in investment on railway infrastructure and a similar growth in investments on rolling stock from 1995/96 to 2005/2006.

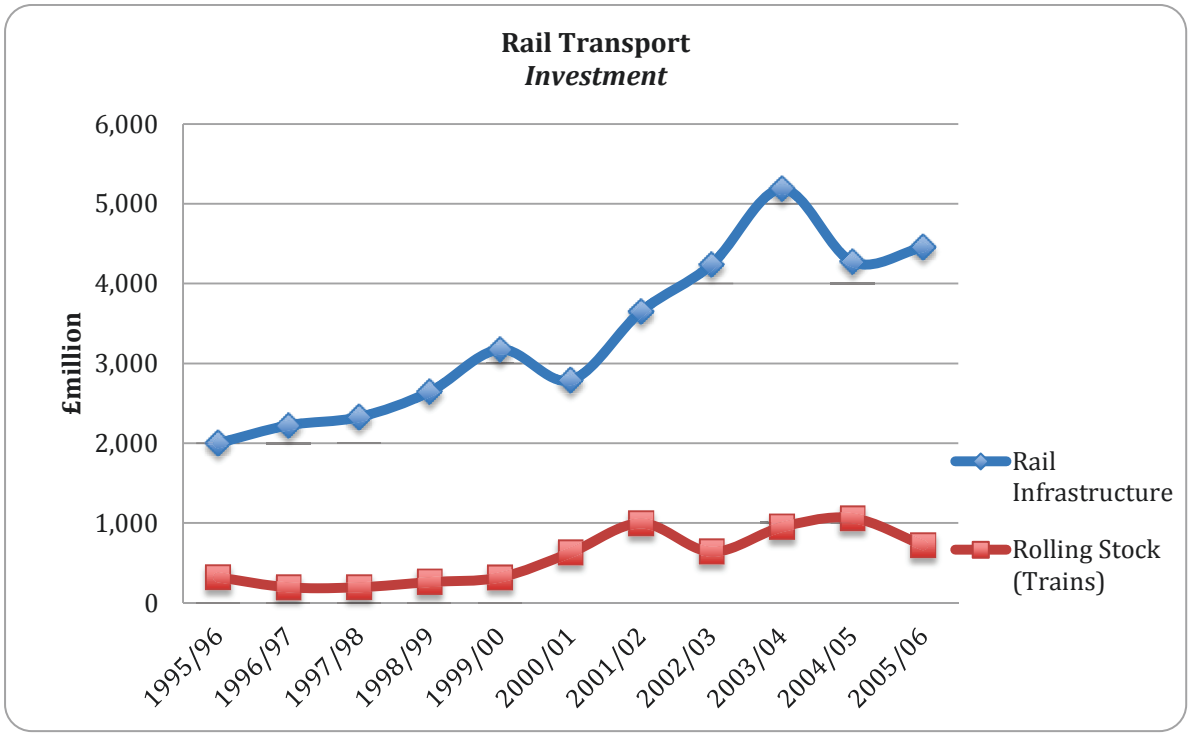


Figure 6: Rail Transport - Investment

Table 6 is based on passenger casualties owing to train accidents and movement accidents. This is the basis for comparisons with other modes of transport. Under the new Accidents Reporting Regulations (RIDDOR 95) brought into force from 1 April 1996, all injuries to members of the public are now reported as either minor injuries or fatalities/death.

Table 6: Railway Movement Accidents: Passenger Casualties and Casualty Rates (Source: DfT 2008)

					Number/rate per billion passenger kilometres						
Casualties	1997/98	1996/99	1999/00	2000/01	2001/02	2002/03	2003	2004	2005	2006	2007
Deaths	22	17	43	17	10	20	8	8	5	4	5
Minor Injuries	807	708	859	788	594	684	637	623	602	545	620
All casualties	829	725	902	806	604	704	645	631	607	549	625
Casualty rates											
Deaths	0.5	0.4	0.9	0.4	0.2	0.4	0.2	0.2	0.1	0.1	0.1
Minor Injuries	19.4	16.2	18.6	16.9	12.5	14.3	12.9	12.4	11.6	9.9	10.6
All Casualties	19.9	16.6	19.5	17.3	12.7	14.7	13.1	12.5	11.7	10.0	10.7

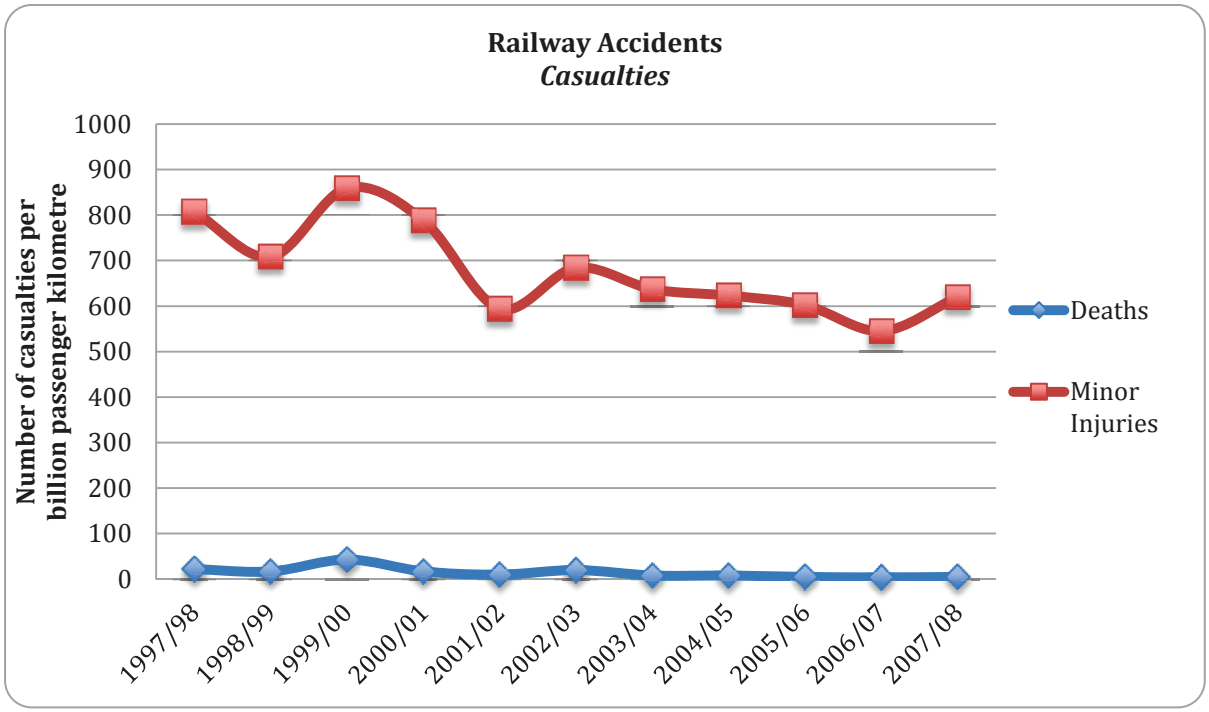


Figure 7: Casualties 1997/98 – 2007/08

The downward trend shown by the reduction in casualties, minor injuries and death over the 10 year period demonstrates the safety improvements made between 1997/98 and 2007/2008 supporting the argument that privatisation has made the railway safer to operate and use.

Table 7 shows the total number of train accidents (collisions, derailments etc.) reported, irrespective of whether personal injury was involved. The figures include accidents on non-passenger lines and those closed to normal traffic while engineering work took place.

Due to European regulations on the reporting of rail transport statistics, the rail accidents data now covers calendar years, rather than financial years. As such, there is overlap between the 2002/03 data and the 2003 data, with accidents from 1 January 2003 to 31 March 2003 reported in both. However, each represents 12 full months.

Table 7: Railway Accidents: Train Accidents (Source: DfT 2008)

	1997/98	1998/99	1999/00	2000/01	2001/02	2002/03	2003	2004	2005	2006	2007
Collisions	127	121	94	106	101	69	61	60	27	20	23
Derailments	93	117	89	93	88	67	63	62	64	46	47
Level crossings & obstructions	680	690	753	693	557	495	433	523	480	503	486
Fires	344	343	340	301	291	292	271	323	187	163	141
Damage to drivers' cab windscreens	619	564	617	607	665	498	409	368	299	328	309
Miscellaneous	0	0	2	1	2	0	0	0	0	1	-
All accidents	1863	1835	1895	1801	1704	1421	1237	1336	1057	1061	1006

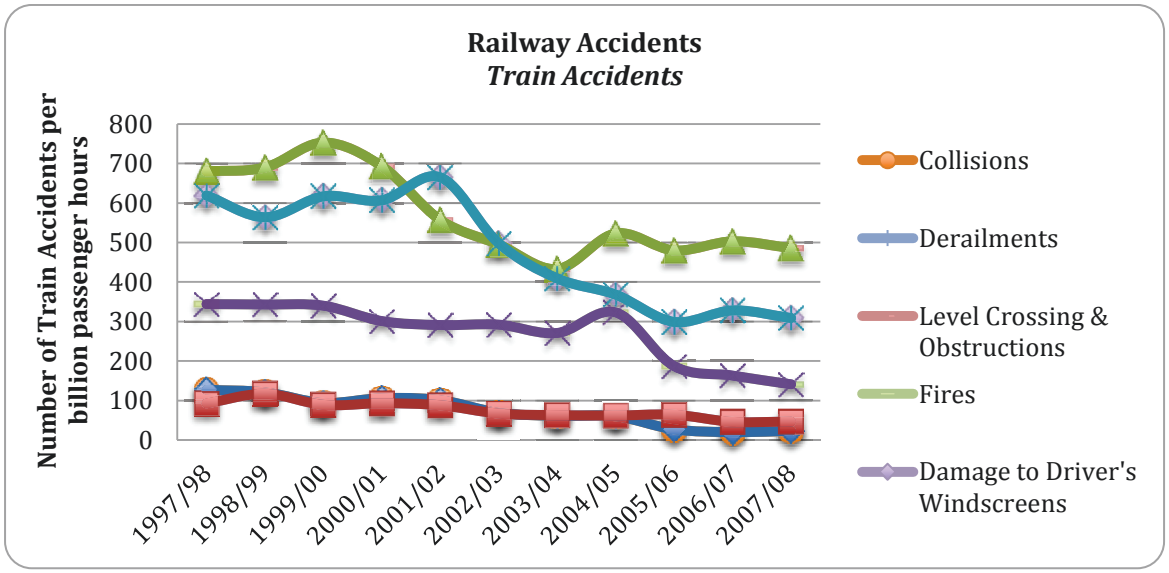


Figure 8: Train Accidents 1997/98 – 2007/08

Figure 8 indicates a downward trend in the different train accidents reported. The total number of reported accidents reduced from 1,863 in 1997/1998 to 1,006 in 2007/2007 demonstrating an 85% decrease in the number of recorded train accidents over the 10 year period.

The tables and charts all show positive trends through the safety improvements made. Investments are generally in the right direction and are having the right effect. As we see the passenger journeys are increasing which strengthens the case for continued funding.

The introduction of the Train Protection and Warning System (TPWS) in 2003 on the mainline railways may have contributed significantly to the reduced number of collisions, derailments and overruns. This thesis does not independently assess the effectiveness of the TPWS but considers in general within the limitations of available data, the overall effect of introduction of Automatic Train Protection Systems (ATP) and other railway safety systems as part of the investments made on improving safety and performance.

Despite this positive trend and growth in the major factors that dictate the direction for future rail systems use and investment, the questions that arise are:

- Are we getting good value for the railway investment projects or for the introduction of new systems, considering the proposals for future renewal projects and new rail projects such as the highly publicised Crossrail and the High Speed 2 (HS2)?
- What confidence do we have that the rail projects, current and future will not only meet performance requirements but also comply with safety regulations?

- What methodologies are available to evaluate safety performance so that decisions made on rail system investments will be well informed and achieve a maximum risk reduction given a fixed budget?

These are challenges faced by the government, rail operators and subcontractors/manufacturers and directly affect both passengers and the general public.

2.5 Review of Major UK Railway Accidents - Lessons Learned.

The evaluation of recent railway accidents (over the past two decades) demonstrates the effectiveness of the press coverage and the abrupt change in the public's attitude to safety. This has invariably led to the intervention of the government, with active investigations and reviews of existing railway structures leading to well-publicised railway reviews and subsequent restructuring.

The high profile accidents that led to these revolutionary railway changes outlined in Section 2.1 are:

- The Watford South Junction train accident on 8th August, 1996;
- The Southall train accident on 19th September, 1997;
- The Ladbroke Grove train accident on 5th October, 1999;
- The Hatfield train accident on 17th October, 2000.

This section provides a brief outline of how all these accidents occurred, but its main focus is the two major accidents, the Southall and Ladbroke Groove train accidents that led to several publications by critics of the government's privatisation policy and to official reports from the Health and Safety Executive for the series of inquiries conducted.

In a joint inquiry into the Southall and Ladbroke Grove accidents, Professor John Uff and Lord Cullen duly noted (HSE 2001a) that '*No one can be unaware of the strength of publicly expressed opinions about current safety issues, whether they concern railways, road traffic, industrial accidents or any other activity which poses a risk to the safety of the public. Equally, anyone who has followed public attitudes for a decade or more cannot be unaware that this is a relatively recent phenomenon. In the past railway crashes, even very major ones, did not produce the level of public reaction which currently results from any rail accident involving casualties. Changes in public attitude have been reflected in, and perhaps influenced by, major changes in the law and practice relating to safety*.'

Since these well-publicised train accidents, a number of studies have been undertaken by HSE and other organisations on behalf of the government. Prominent amongst these are the primary inquiries that led to the recommendations discussed in this section. Such studies include the inquiry into the Southall Rail incident (HSE 2000a), HSE investigation into the train collision at Ladbroke Grove (HSE 2000a), the

Ladbroke Grove Rail reports for the Phase 1 and 2 inquiries (HSE 2000c, HSE 2001a), the Southall and Ladbroke Groove Joint Inquiry into the Train Protection Systems (HSE 2001a), study on Automatic Train Protection (RAE 2000), the assessment of Railtrack's management of multi-SPAD signals (HSE 2002), study on the management of safety in Railtrack (HSE 2000d) and finally a report on the progress of recommendations on the above mentioned reports and studies.

The Southall collision was the first major accident to occur within the UK rail network since its privatisation, which formally started with the transfer of the railway infrastructure to Railtrack on 1 April 1994.

The Southall rail accident took place at Southall East Junction on 19 September 1997 when the 10.35 high speed train from Swansea to London Paddington, operated by Great Western Train Company, was in collision with a freight train operated by English Welsh and Scottish Railway as it was crossing to Southall Yard. Seven people died and a further 139 people were injured, some severely.

The inquiry into the Southall Rail Accident was led by Professor John Uff. The purpose was to determine why the accident happened, to ascertain the causes, and to identify any lessons which have relevance to those with responsibilities for securing railway safety and to make recommendations.

Brief accounts of the Watford South Junction and Hatfield train accidents are documented in Beale (2002). In the former, a passenger train passed a signal at danger and collided with an empty coaching stock train. One passenger was killed; sixty nine passengers required hospital treatment and four train crew workers suffered injuries. The key factors included:

- The risk of human errors causing SPADs (Signals Passed At Danger) and technological options for reducing these risks with Automatic Train Protection (ATP) systems;
- Confusion caused to train drivers due to a speed restriction sign being placed in an inappropriate position and the ambiguity in the railway signalling standard which contributed to the problem;
- The shorter than normal safety margin for the signal that was passed at danger.

In the case of the Hatfield train accident on 17 October 2000, a high speed passenger train was derailed when a section of damaged rail broke. Four passengers were killed and 70 people were injured, including four seriously injured. Large sections of the UK rail network were affected by subsequent track closures and speed limits as similar sections of track were investigated. This caused transport chaos in the UK and led to the resignation of the Chief Executive of the rail infrastructure company. The key factors associated with the accident were:

- Management and maintenance of the rail infrastructure and the systems for detecting and correcting fatigue cracks in rails;
- The long delays in responding to identified cracked rails;
- The fragmentation of the industry and resulting difficulties in completing essential work quickly when multiple independent organizations are involved, each with their own priorities and bureaucracy.

The four major public inquiry reports were as a result of the two train crashes mentioned above.

Professor Uff was appointed to chair the Public Inquiry into the Southall crash and published his report in February 2000, with 93 recommendations. Lord Cullen was appointed to chair the public inquiry into the Ladbroke Grove crash, which he held in two parts: the Part 1 report (HSE 2000c) concerning the train crash was published in June 2001 with 89 recommendations, and the Part 2 report (HSE 2001b) relating to wider issues of safety management and the then current regulatory regime was published in September 2001 with 74 recommendations. The Joint Inquiry into Train Protection Systems was established shortly after the Ladbroke Grove crash and during the course of the Southall Inquiry. Professor Uff and Lord Cullen acted as joint chairmen.

Unusually, this Public Inquiry was not concerned with the facts of either crash but with broader questions relating to train protection and warning systems and measures to prevent or reduce the risks of signals being passed at danger. The Inquiry report was published in March 2001 with 39 recommendations.

The Public Inquiries led by Lord Cullen and Professor Uff took a fundamental look at the rail industry and examined in detail its generic safety issues. The Government agreed that the 295 recommendations from the four Public Inquiry reports established a convincing, necessary and challenging agenda for change. The scope of the Inquiry recommendations covered specific detailed technical issues to underlying conditions of culture and management practice. Some are still fundamental to achieving overall improvements in the state of the industry's safety management, whilst others are less wide ranging.

Table 8: Inquiry Findings and Recommendations

Significant Inquiry Findings and Recommendations (Southall and Ladbroke Grove)	**Notes / Source**
Driver Training - The most important lesson to be learned, in terms of driver training, is that while passenger safety continues to depend on the vigilance of drivers, and while SPADs continue to occur at a rate of around 2 per day, efforts must concentrate on all possible means of ensuring that drivers act with the maximum of vigilance and responsibility, and that any potential for irregular behaviour is eradicated. Further research should be carried out to develop the understanding of human factors as they relate to train driving. Signallers and drivers should jointly attend away days and other training	Applied to both Southall and Ladbroke Grove. Extracts from the HSE (2000a). The Southall Rail Accident Inquiry Report and HSE (2000c) - the Ladbroke Grove Rail Inquiry. Part 1 Report

Significant Inquiry Findings and Recommendations (Southall and Ladbroke Grove)	Notes / Source
processes to develop their mutual understanding.	
Licensing – There should be a system for the licensing and central recording of those who are qualified for the driving of trains in respect of their knowledge of the rules and regulations and the traction for which they have been assessed as competent. Training providers or train operators should be accredited and common standards laid down for the purpose. Drivers' licences should require to be revalidated every three years. There should be a similar system for licensing the central recording of qualified signalmen, based on an assessment of their knowledge of the rules and regulations. Revalidation every three years should be required.	Ladbroke Grove Rail Inquiry HSE (2001b). Part 2
Operating Rules - sections of the Rule Book and Group Standards which were examined and highlighted revealed an appalling lack of clarity relating particularly to Automatic Warning Systems (AWS) isolation.	Southall. HSE(2000a)
Fault reporting - the Southall accident revealed widespread failures of compliance with fault reporting procedures. This included lax performance by individuals of tasks which, at the time, they had no particular reason to regard as significant (but which acquired very high significance in the light of the accident). It revealed also failures to put in place systems that were likely to perform adequately when called upon. The lesson to be learned seems to be that compliance with Rules cannot be assumed in the absence of some positive system of monitoring which is likely to detect failure.	Southall. HSE(2000a)
Fleet maintenance - The major lessons to be learned from the experiences of the Southall crash is that potentially serious deficiencies may develop in detailed maintenance procedures which are not detected by conventional management procedures or by audit. Most surprising was the fact that management was apparently unaware of the unsatisfactory procedures which existed, both in terms of comprehensible maintenance procedures and equipment for the repair of reported AWS fault.	Applied to both Southall and Ladbroke Grove
Infrastructure maintenance - Lessons to be learned in regard to the rail infrastructure are limited to the signals, where 2 out of 3 vital signals were found to be substantially misaligned, one being grossly misaligned. This revealed that errors must have occurred at the stage of installation which were not picked up by routine maintenance during the period of well over 2 years that they were in use before the Southall crash; nor in the period of some 18 months after they were handed back into normal maintenance. The failure to detect misalignment after installation shows that no adequate testing could have been performed at the time of commissioning.	Applied to both Southall and Ladbroke Grove
Regulation - The lesson learnt in relation to regulation is that not all changes have safety implications.	Applied to both Southall and Ladbroke Grove
Vehicle design and operation - The lessons to be learned in relation to crashworthiness were limited to questions of emergency access and procedures. The Southall crash revealed serious deficiencies in the means of getting out of a coach on its side, with lighting no longer functioning and internal doors jammed. Recommendations included a number of issues raised in relation to the operation of vehicles.	Southall
Research and Development - An important lesson learnt from a number of different aspects of the Inquiry proceedings is the inability of the rail industry to deal effectively with inter-company issues.	Applied to both Southall and Ladbroke Grove
Automatic Train Protection - the lesson from the technical experiences of the ATP project was that the industry was over-optimistic both in terms of the time necessary to develop the new systems and the cost involved. In an industry based on privately raised finance, projections must be realistic and results must bear proper comparison with predictions. On the positive side, ATP was nearing formal acceptance. Its very high level of use represented a major safety advance on those	Southall

Significant Inquiry Findings and Recommendations (Southall and Ladbroke Grove)	Notes / Source
sections of the Great Western lines fitted with ATP.	
General Safety Issues - the difference between appearance and reality in terms of the commitment to safety and systems intended to achieve safety. An important lesson to be learned from the Southall crash is that the difference persists and had not diminished in any way in its potency to mislead and create false assurance.	Applied to both Southall and Ladbroke Grove
Accident investigations and inquiries- A thorough review of the process is urgently called for. The lesson learnt from the Southall crash was that accident investigation was not rendered more effective by duplicated and partial procedures. The reverse was the case. At Southall, unregulated and competing interests succeeded in duplicating and confusing both the investigation and inquiry.	Applied to both Southall and Ladbroke Grove
Post-accident procedures - lessons are to be learned, however, in relation to a number of procedures which did not operate as they should have. These have generally been identified and improvement can be expected.	Applied to both Southall and Ladbroke Grove
Safety Auditing - The safety audit process should be strengthened, and the quality of communication during the process should be improved.	HSE (2000c). The Ladbroke Grove Rail Inquiry. Part 1 Report.
Signal sighting - The standard on signal sighting should require that explicit consideration is to be given to the readability of a signal. The standard on signal sighting should deal explicitly with the additional time required for the reading of certain signals, including (but not necessarily limited to) those mounted on gantries The standard on signal sighting should define acceptable limits to the temporary obscuration of a signal, subject to the overriding right of a signal sighting committee to determine whether the nature and extent of the interruption in the individual case is such that the sighting is unacceptable. Signal sighting should form part of Railtrack's safety management system that it is the responsibility of senior Zone operating and signal engineering management to decide whether the recommendations of a signal sighting committee under the Group Standard on SPADs are to be implemented and, if not, what alternative measures are to be taken, and relevant measures are implemented.	Extracted from HSE 2000c. Applies to both Southall and Ladbroke Grove
SPAD - The Group Standard on SPADs and its associated documentation should be reviewed to ensure that there is no presumption that driver error is the principal cause, or that any part played by the infrastructure is only a contributory factor. Persons who investigate, and make recommendations as a consequence of SPADs should be trained in the identification of human factors and in root cause analysis. Their competence in these areas should be formally recorded and developed by refresher courses. The analysis of SPAD data should be specifically directed to eliciting the part played by human factors and assessing the significance of the hazards.	Applied to both Southall and Ladbroke Grove
Signallers' Training and Instructions - The instructions for signallers as to their response to a SPAD should be clarified; and set out in a single set of instructions, while if there are matters which are specific to a particular area they should be covered by separate local instructions. Railtrack should institute a system whereby all signallers in the signal box (or centre) are briefed by their line manager following a SPAD in their area, and there is appropriate dissemination of information which may be of assistance to signallers elsewhere.	Applied to both Southall and Ladbroke Grove
IECC equipment - There should be a unique alarm for SPADs, which should sound until it is turned off. The speed with which signallers can take action to move points in an emergency should be improved.	Applied to both Southall and Ladbroke Grove

Significant Inquiry Findings and Recommendations (Southall and Ladbroke Grove)	Notes / Source
Automatic controls - There should be a study of the possibility of the automatic replacement of a signal to Danger where a SPAD has occurred and the layout is such that there is a significant danger of collision	Applied to both Southall and Ladbroke Grove
Radio Communication - There should be a national system of direct radio communication between trains and signallers.	Applied to both Southall and Ladbroke Grove
Preservation of data - Signallers, managers and maintenance staff working at IECCs should be instructed as to the need to preserve CSR data disks in the event of a SPAD taking place.	Applied to both Southall and Ladbroke Grove
Crashworthiness - The enhancement of the cabs on HSTs to improve driver protection along with energy absorption and compatibility with other vehicles, and the enhancement of measures for the retention of bogies on the coaches of HSTs, should be considered, subject to an assessment of feasibility, costs and benefits, with a view to a possible retro-fitting.	Applied to both Southall and Ladbroke Grove
Fire mitigation	Ladbroke Grove Report 1
Passenger protection, evacuation and escape	Applied to both Southall and Ladbroke Grove

The Ladbroke Grove train crash on 5 October 1999 resulted in 31 people losing their lives and with over 400 injured. Part 2 report of the Ladbroke Grove Rail Inquiry HSE (2001b) makes additional recommendations on the following vital elements of safety management, including:

- Research and development
- The use of contractors
- The role of the trade unions
- Safety leadership within individual companies
- Communications – two way communications between management and the workplace
- Risk assessment - the greater use of risk assessment in the rail industry was commended
- Railway Group Standards
- Safety cases – endorsed the application of safety cases to the railways
- The accreditation of suppliers and producers of services
- Railtrack and Railway Safety
- The safety regulator – HMRI to continue to fulfil the function of the rail regulator
- Accident investigation - The responsibility of the HSE for the investigation of rail accidents should be transferred to an independent body, RAIB.

The assessment of the management of multi-SPAD signals was the result of the collision between two trains at Ladbroke Grove. The purpose was to assess the effectiveness of Railtrack's systems for avoiding the risks arising from signals passed repeatedly at danger (multi-SPAD signals). The report contains

examples of the measures taken, or planned, at a number of specific signals to reduce the likelihood of further SPAD incidents occurring.

Following the Ladbroke Grove train accident, David Davies (RAE 2000) examined the consequences of SPADs and recommended ways to minimise their effects including evaluating *options for train protection*. The report argues that although less than 1% of SPADs lead to accidents, they remain an area of serious concern for railway safety. The SPAD phenomenon occurs in other countries; however, comparative statistics were not available owing to differences in signalling systems and data collection. More research on human factors and driver operation was strongly recommended, augmented by an urgent programme of fitting enhanced forms of train protection. Davies made long, medium and short-term recommendations which were wholly adopted during the inquiry on the Ladbroke Grove accident:

- Longer term - Railway policy and implementation should aim at the European Railway Train Management System/European Train Control System (ETCS) as the best way forward.
- Intermediate future. Using the criteria of maximising safety by minimising the probability of SPAD related accidents over the next 10 to 15 years; this report concludes that the best solution (irrespective of cost) is to fit the Train Protection and Warning System.
- Short term – As a result of the operational risks of relying on the TPWS, considering its known failures (i.e. 70% effective in terms of avoiding ATP preventable accidents for trains travelling above 75mph), it was recommended that a small pilot trial of a variant of TPWS called TPWS+ should be set up.

The joint inquiry into the Southall and Ladbroke Grove Train Protection Systems (HSE 2001a) comes between the report into the Southall rail accident, and the report into the Ladbroke Grove accident. The report is not concerned with the facts of either accident, but with broader issues of safety on the railways in order to track developments following the accidents. This report reviews and assesses the value of all train protection systems which were currently or shortly to be available, and considers other means of preventing signals being passed at danger or of mitigating the effects.

The management of safety in Railtrack HSE (2000d) is a report of the review of safety management arrangements within Railtrack carried out by HSE. In summary the key areas for attention as recommended were:

- Railtrack could enhance its leadership role within the Railway Group by leading the development of Group Standards for key safety management system processes such as investigation, inspection and audit;

- Railtrack could improve the way it seeks to secure Train Operating Companies' (TOCs) compliance with their safety cases by:
    - Expanding the scope and nature of monitoring TOC performance, particularly at Railtrack Zone level;
    - Clarifying what constitutes unacceptable TOC performance and the means for securing remedial action;
    - Improving the co-ordination of activity and information on TOCs collected by Railtrack's Safety and Standards Department and Railtrack Line.

Other important recommendations from this report include proposals for enhancing safety management within the Line, by improving:

- The performance criteria for the key components of its safety management system;
- The use of risk assessment both in establishing performance criteria and in proportionately allocating resources and prioritising safety management actions;
- Active monitoring at corporate and Zone level by developing key performance indicators which enable an assessment of overall performance and permit real time re-allocation of resources according to emerging needs;
- Investigation of accidents and incidents to establish underlying causes and consistent, comprehensive analysis of common causes and trends; auditing so that activity is targeted at need, co-ordinated across the organisation, reported in a helpful style, audit actions closed out speedily, and underlying causes analysed to achieve continuous improvement;
- The information for review to enable an overall corporate picture of performance to be gauged so that better strategic decisions can be taken;
- External benchmarking with other high hazard industries on safety management system documentation processes and safety culture as an aid to learning and continuous improvement in safety management practice.

Progress reports were produced by the Health and Safety Commission to demonstrate that the recommendations had been implemented. A final report from the Health and Safety Commission (HSE 2005) showed some progress on the implementation of the 295 recommendations from the four public inquiries. This report, tenth in the series, confirmed that the public inquiries delivered results.

Almost all the recommendations including recommendations in Table 8 have been implemented and the cited report shows the progress with the remaining recommendations. The key remaining

recommendations (continuing beyond 2005, date of the progress report) that require completion are summarised below:

- Undertake pilot schemes using the European Train Control System (ETCS)
- Advance selective fitment of the GSM-R radio prior to introduction of the ETCS
- National system of direct radio communication – trains and signallers
- Supply chain management and accreditation of contractors i.e. suppliers of safety-critical products or services.

Whilst the four railway accidents identified earlier shaped the future of the UK railway industry, the Potter's Bar railway accident, another significant derailment accident that occurred in May 2002 (ORR, 2002) was instrumental in supporting the urgent need to implement existing recommendations from previous accidents. The rear coach of the passenger train derailed after passing over a set of points just outside the Potters Bar station. The derailment led to the loss of 7 lives and injuries to over 70 people. The independent investigation board set up under the Health and Safety at Work etc. Act 1974 produced three reports into the accident and recommendations presented in ORR (2003). The Investigation Board was disbanded in 2008 following closure of all outstanding recommendations.

Chapter 3 Risk Assessment and Risk Management in the UK Railway Network

This chapter focuses on the likely scenarios or primary factors that could lead to uncertainties and diminishing confidence in the current risk assessment techniques, tools and practices. The first section also presents robust reasons why careful considerations are required before using quantified risk assessments that are now a standard tool for predicting targets and desired system performance in the railway industry. It also establishes the influence of assumptions in determining whether the results achieved are realistic or not. It is also now widely accepted by engineering managers, project managers, risk analysts and railway industry decision makers that uncertainties are inevitable. Will they always exist in the quantified risk assessment models? To what extent – if any; is this acceptable?

The application and associated complexities of the concepts, tools and techniques such as failure identification methods, Precursor Indicator Model (PIM), Safety Risk Model (SRM), Fatalities and Weighted Injuries (FWI), classic risk equations, F-N curve, currently used to quantify risks are comprehensively discussed. This chapter finds that the one of the key fundamental challenges with the methods currently practiced is that they do not model the root causes of failure and the quantification of many of the events in the high consequence/low frequency categories such as train collision are based on very few past incidents and as such under-represented. This chapter lays the foundations for the concepts and methods introduced in future sections of this thesis as it identifies two basic errors often ignored during risk analysis i.e. over-estimation and application of empirical data from older systems which may not apply to newer systems with improved standards.

3.1 Existing Techniques and Tools for Risk assessment and Risk Management

On the mainline railways, introduction and implementation of the appropriate risk assessment techniques and tools for the distinct applications is a challenge and has significant cost implications. Introducing a not-for-purpose tool is in most cases more expensive than doing nothing - with incorrect assessment and subsequent costs of failure potentially catastrophic. However, in the UK railways, these decisions are guided by the Health and Safety at Work Act 1974 and the ALARP criteria.

Guidance and standards in the UK railway industry for conducting risk assessment is given in Figure 9.

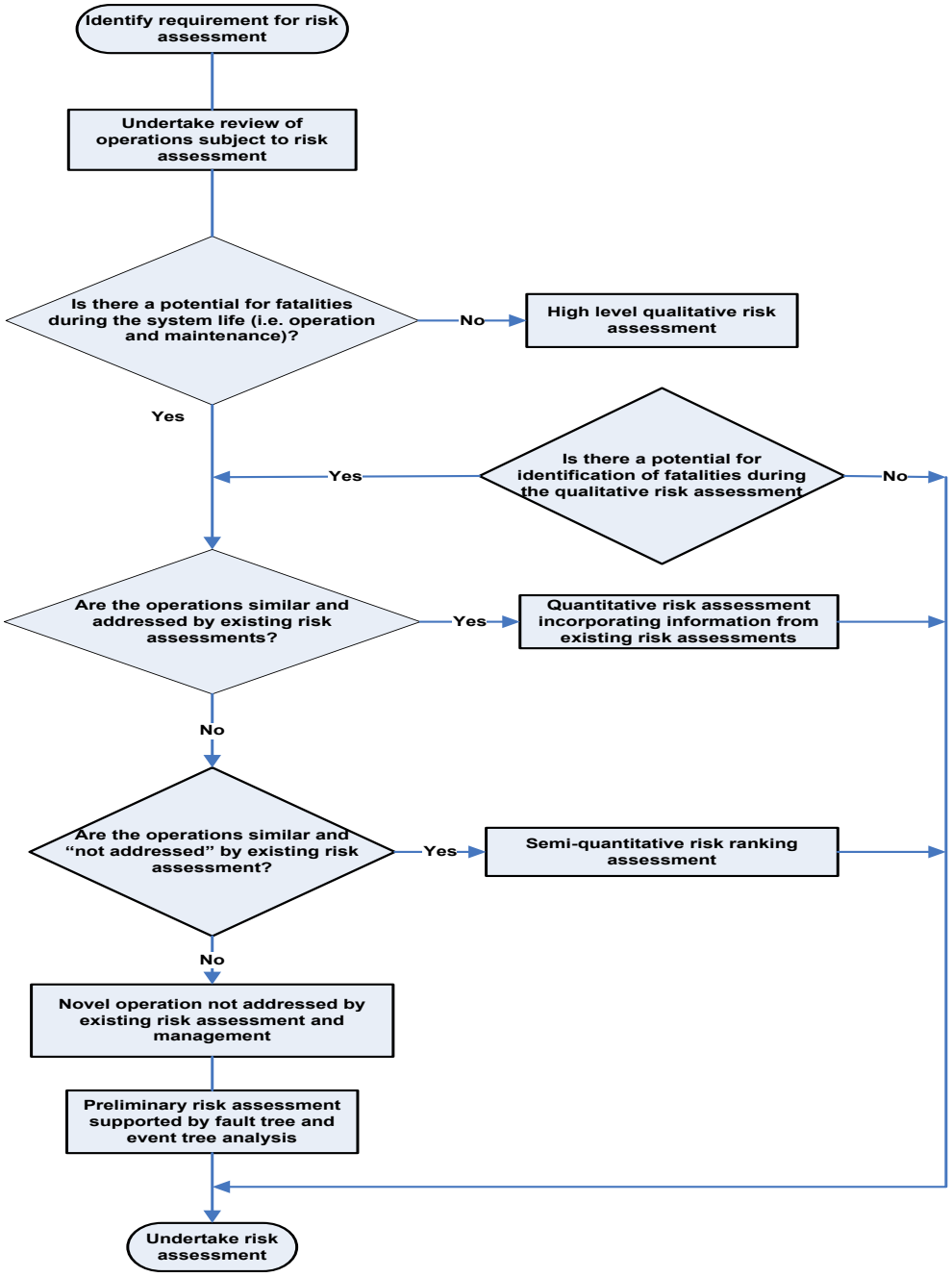


Figure 9: Guidance on selecting the most appropriate risk assessment methodology

The application of classical safety analysis is hindered by the increasing complexity and corresponding cost of railway systems. Fault trees and Failure Mode Effects Analyses are manageable for relatively simple systems. These conventional methods can quite easily become laborious and error prone, further making thorough assessment and interpretation of the results increasingly difficult within the time and budget constraints of most railway undertakings. Furthermore, the results of the analyses are divorced from the design being analysed, so that the effects of any changes in the system design may only become apparent after another long and costly analysis.

With this in mind, this section looks at alternative methods that have been introduced on the railways. On mainline routes, the underlying risk of train accidents is measured by tracking changes in the occurrence of accidents using the Precursor Indicator Model (PIM). The PIM was first developed in late 1999 and has since been modified effectively. RSSB (2010) presents complete details of the PIM, with a comprehensive guide on its structure, usage and benefit. The PIM monitors the risk from train derailments, train collisions, buffer stop collisions, train fires and trains striking road vehicles at level crossings. The precursors covered by the PIM fall into six main groups, encompassing 28 separate subgroups and 46 lower level groups. The irregular working and SPAD components of the PIM model were updated in early 2010 to incorporate risk ranking information.

The PIM monitors train accident risk to passengers, the workforce, and members of the public, such as motorists on level crossings. The PIM value is an annual moving average, so it reflects precursors during the previous 12 months. It is also normalised by train miles, to account for changes in the level of activity on the railway. The PIM uses the classic risk Equation 2.1 presented in Section 2.4 where risk is a function of the frequency of the event and consequence.

Frequency estimates are based on accident precursor data; consequence estimates are derived from the Safety Risk Model (SRM). The SRM models hazardous events (i.e. those that could lead to harm on the railway). Each is broken down into the precursors that could lead to its occurrence. The risk associated with each hazardous event and its precursors is estimated, and the results presented in terms of Fatalities and Weighted Injuries (FWI) per year. The SRM provides an estimate of the risk at a particular point in time and is updated periodically. Each month, the number of occurrences of each accident precursor is multiplied by the average consequences per event for that precursor (as estimated by the most recent version of the SRM) to give an estimate of the associated risk to be used in the PIM. The risk from all precursors over the previous 12 months is then summed and normalised per million train miles. The normalised figures are subsequently validated against the annual average using a previous

standardised model.

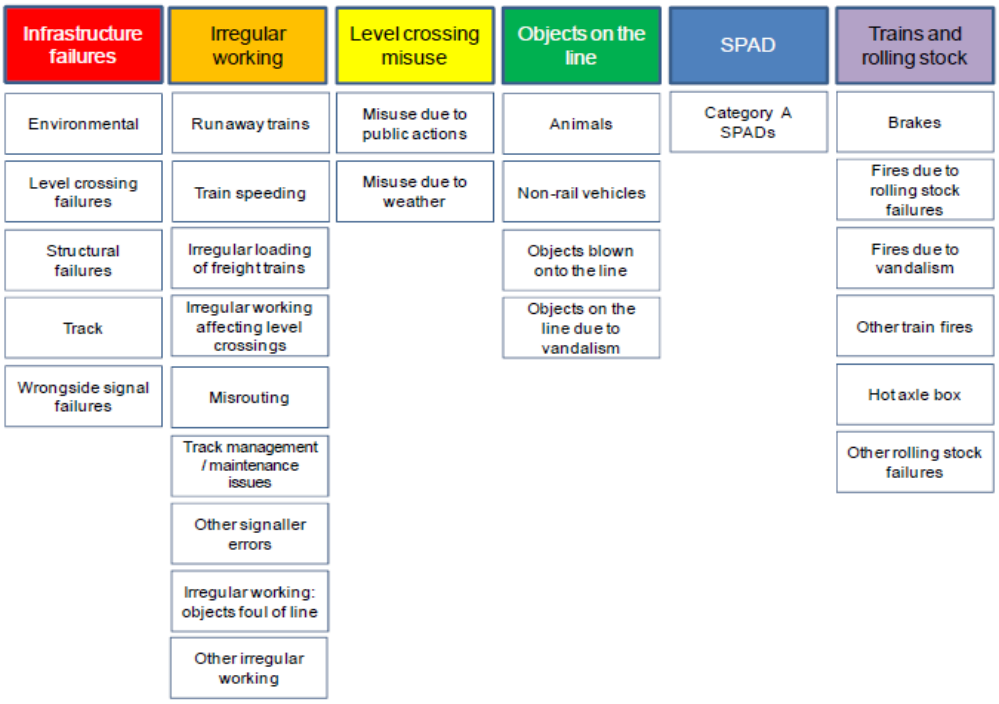


Figure 10: PIM Structure (Source: RSSB 2010)

Train accident risk estimates from the SRM are used to measure performance against the High Level Output Specification (HLOS) safety metrics but the PIM provides interim information on trends in train accident risk.

The PIM only analyses train *accident* risks. As a complete railway risk assessment tool, the PIM is limited in its application. Movement/Non-movement risks as defined by the SRM are not within the scope of the PIM, making it a very expensive tool considering that train accidents account for a relatively small part of the overall railway system risks. In using the PIM, it is assumed that accidents can be accurately predicted and avoided by simply acting on the predictions from models that employ PIM information.

Perrow (1999) argues that accidents are inevitable in any system of sufficient complexity. However, this assumption, built into the PIM indicates a limitation in the use of accident precursor models as it currently under represents the reality of accidents. The PIM relies on incident reporting from the Safety Management Information System (SMIS). As with most safety models in current use, the incident reporting schemes are subject to several potential flaws. Reporting bias and under-reporting can undermine the veracity of the data and the danger that these schemes have significantly over-estimated the impact they can have on the operation of complex, safety-critical systems (Johnson 2002). The challenges with data quality used in prediction models are introduced in Section 2.3 and addressed in detail in Chapter 4.

F-N (F – frequency of occurrence; N – number of fatalities or persons harmed) curves or criterion lines have been used in various countries and in various contexts for over 30 years. Ball and Floyd (1998) reviewed the use of F-N curves for the HSE for risk target setting. The HSE does not explicitly recommend the use of F-N curves in this area. However, the HSE document Reducing Risk Protecting People (HSE, 2001c) cautiously recommends at least an F-N-criterion point. On an F-N criterion, if a system under investigation using F-N curves generates lines that lie wholly below the criterion line, the system is regarded as tolerable. Safety measures to lower the F-N curve are then required.

The Railway Safety's Safety Risk Model (SRM) provides in the Risk Profile Bulletin (Railway Safety 2003) an F-N curve for multiple fatalities railway accidents. The F-N curves from Railway Safety covers train accidents with the potential for multiple fatalities with data derived from modelling the precursors and consequences of fatal accident sequences. The categories modelled include:

- Train derailments
- Collisions
- Overruns
- Collisions between trains and road vehicles (mostly at level crossings)
- Train fires

These are collectively considered as train accidents. It is worth noting that other non-train accidents such as station fires were not taken into consideration in generating the SRM but also have a potential for causing multiple fatalities. Risk reduction at level crossings has been a significant challenge to policy makers, railway infrastructure owners, operators and contractors. HC (2014) provides that the safety record of Great Britain's level crossings has improved in recent times however also highlights that nine fatalities, seven major injuries, fifty-three minor injuries and seventeen cases of shock or trauma were reported in 2012-13. This generally accounted for half of the fatalities on the UK railways in the period from 2008-09 to 2012-13.

Andrew W. Evans (2005) reviewed railway risks between 1967 and 2001, focusing on fatal collisions, derailments and overruns on running lines of the UK national railway system. The results, based on empirical data as part of a NERA report, was used by the Office of Railway Regulation as a suitable comparator for the SRM F-N curve for all main train accidents in 2001. The report indicated that for much of its length, the SRM F-N curve is above the empirical curve.

The estimates of the SRM tend to be higher than those attained directly from accident data partly because the SRM curve has a wider coverage. However, the NERA report discovered that the two curves come close together at the high fatality end of the range (i.e. 50 – 100 fatalities). The SRM curve

continues above the 100-fatality level to include the possibility of accidents larger than any that have been recorded or have occurred in Western Europe in the last 35 years. At this level, the frequencies reach such insignificant levels that the overall risk is negligible. Despite these differences, Railway Safety believes that the curve is an accurate representation of the SRM for frequencies of accidents with 5 or more fatalities.

It can be argued that the use of empirical data may not be adequate in setting F-N criterion for accidents/fatalities because of the weakness of available main-line train accidents data. There were 3 accidents with more than 20 fatalities between 1967 and 2001. This means that an estimation of the train accidents on the FN curve will only be adequately generated at the upper end of the fatality distribution from British operational railway accident data.

Evans and Verlander (1997) undertook research into the use of the F-N criterion lines and considered them inconsistent. Their objections included:

1. FN-criterion lines were conceived as an analogy to individual risk criteria. The justification for individual risk criteria is essentially equity: it is unfair to impose too high risks on particular individuals, whatever the benefits may be. However, there is no corresponding equity argument for accidents as distinct from individuals and therefore the analogy is false.
2. Even if limits to the tolerable frequencies of accidents of different sizes were desirable, they would need to be based on clear and preferably empirically derived criteria. There are at present no such criteria.
3. Even if such criteria could be derived, FN-criterion lines are a technically incorrect method of implementing them, because they do not meet the requirements for consistency in decision making under uncertainty.

The shortfalls in the use of conventional risk assessment tools for system safety applications such as fault trees and failure modes and effects analysis techniques led to an emergence of automated risk assessment tools in the 1990s. These developments and the application of new risk assessment tools to replace them have been in and out of the industry largely due to the lack of investment to enhance them for use in the railway industry. In short, these risk assessment tools were simply not modifiable for complete system risk analysis and evaluation, or for system optimisation. As a result, the railway application limitations made them practically unusable.

Other risk assessment tools and novel techniques have been introduced to the railway industry from other high hazard industries. Some that are undergoing pilot studies and application test runs but have not yet been accepted include:

- The Functional Resonance Accident Models (FRAM).
- The Hierarchically Performed Hazard Origin and Propagation Studies (Hip-HOPS).
- Failure Propagation and Transformation techniques such as the Failure Propagation and Transformation Notation and the Failure Propagation and Transformation Calculus (FTPN and FTPC)
- State Event and Component Fault Trees

Papadopoulos et al. (2011) present the Hierarchically Performed Hazard Origin & Propagation Studies, a computerised system safety analysis tool developed to meet the challenges of the application of rule-based design and classical safety and reliability analysis techniques that are common with new railway system technologies. The tool addresses the introduction of complex failure modes associated with new railway system technologies that are increasingly difficult to analyse by using classical manual system analysis. This key feature is claimed to resolve the challenges of related errors in the analysis. The central capability of this tool is the automatic synthesis of Fault Trees and Failure Modes and Effects Analyses by interpreting reusable specifications of component failure in the context of a system model. The analysis is largely automated, requiring only the initial component failure data to be provided, therefore reducing the manual effort required to examine safety. At the same time, the underlying algorithms can scale up to analyse complex systems relatively quickly, enabling the analysis of systems that would otherwise require partial or fragmented manual analyses. HiP-HOPS employs genetic algorithms to evolve initial non-optimal designs into new versions that better achieve reliability requirements at minimal cost. By selecting different component implementations with different reliability and cost characteristics, or by substituting alternative subsystem architectures with more robust patterns of failure behaviour, many solutions from a large design space can be explored and evaluated quickly.

HiP-HOPS is prone to combinatorial explosion. The system cannot be effectively applied to optimise design (and associated cost) as it uses computationally expensive meta-heuristics. It is highly reliant on the integration of simplified forms of safety and reliability analysis techniques and tools such as Fault Tree Analysis. The tool is relatively new and its use has only been illustrated by using case studies from the shipping industry.

Fenelon and McDermid (1993) present the Failure Propagation and Transformation Notation (FPTN). This is a graphical description of the failure behaviour of a system. FPTN is developed with the concept of describing the generation and propagation of component failures in a given system using component modules. These are connected via inputs and outputs to other modules, allowing combination and propagation of failures from one module to another, and they can be aggregated into subsystems in order to build a system hierarchy. FPTN was designed to provide a bridge between the deductive FTA

and inductive FMEA processes, allowing both cause and effect to be studied. However, FPTN's component-module approach requires building an error model that is separate from the system model, which is then prone to becoming desynchronised from the original system it represents as the design evolves. The Failure Propagation and Transformation Calculus is an advancement of the original FPTN but lacks the capability to achieve the required risk assessment and system optimisation analysis that would assist the decision maker on system options to maximise risk reduction.

Details of the State-Event Fault Trees (SEFTs) and Component Fault Trees (CFTs) are documented in Ge et al. (2009), Kaiser et al. (2007), Grunske and Kaiser (2005) and Grunske and Neumann (2002). These were developed from the FPTN series. CFTs are less prone to combinatorial explosions that affect the FPTN, FPTC and HipHOPS because they are developed based on fault trees and have the capability to build very large component fault trees via a system hierarchy for overall system analysis. Papadopoulos et al. (2011) note that SEFTs are better suited to analysing software systems or hardware systems with more complex dynamic behaviour due to the ability to distinguish between a system being in a certain state (which is a condition that is true over a period of time) and an event that triggers a state transition (which is an instantaneous occurrence). Failure behaviour is modelled at the component level, but the simple Boolean logic of FPTC is extended to enable the representation of sequences and histories of events, as well as the concept of negation (i.e., an event that has not yet happened) using the NOT gate. However, this more complex logic means that analysis of SEFTs is not possible using traditional FTA algorithms, but relies on a conversion to Deterministic Stochastic Petri Nets (DSPNs). These DSPNs can then be quantitatively analysed using Petri Net tools like Time-NET. The disadvantages of modelling different states are the difficulties in applying sensitivity techniques and the fact that the state-space can grow exponentially in larger models, reducing the scalability of the SEFT approach. This further significantly reduces the effectiveness of the system in applying a reasonable degree of sensitivity analysis.

3.1.1 UK Regulatory Framework, Risk Acceptance Criteria and Risk Targets

The provisions of safety following the initial directives that were established as the first steps towards regulation and opening up of the European railway transport market were insufficient. Significant differences between safety requirements were unresolved. These directives, now superseded were:

- The European council directive 91/440/EEC of 29th July 1991;
- The council directive 95/18/EC of 19th June 1995 on the licensing for railway undertakings;
- The directive 2001/14/EC of the European Parliament and Council of 26th February 2001 on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification.

The need to harmonise the content of safety rules; safety certification; roles/responsibilities of safety authorities and investigation of railway accidents led to the establishment of The European Railway Safety Directive (2004/49). The Directive 2004/49/EC has been amended by Directive 2008/57/EC and Directive 2008/110/EC.

The directives establish a common framework for railway safety as a means of eliminating the differences in principles, approach and culture that made it difficult to break through technical barriers between European Member States and establish national transport operations. It is clearly understandable that the directive's key concepts and structures such as Safety Management Systems, Safety Cases (Certificates), Safety Targets (Objectives) and a safety authority (Office of Rail Regulation) were aligned to the UK regulatory and enforcement policies at the time of establishment, due to the railway privatisation and restructuring phases that the UK railway had undergone. Despite the similarities with the existing UK regulation, the differences required resolution which led to the transposition of the European Railway Safety Directive (RSD) 2004/49/EC into UK legislation via the Railways and Other Guided Transport Systems (Safety) Regulations 2013 (ROGS).

The Safety Directive specifically requires, as interpreted and summarised by the Railway Safety and Standards Board (RSSB Europe Safety Management 2011) that:

- Railway companies are responsible for the safety of their part of the railway system;
- The European Rail Agency (ERA) is responsible for harmonising safety standards and requirements through the development of Common Safety Targets (CSTs) and Common Safety Methods for the railway system.

Common Safety Indicators (CSIs) and Common Safety targets (CSTs) were developed to help ensure consistency in the measurement, application and benchmarking of safety levels across Europe. Common Safety Targets are minimum safety levels for different parts of the system and are expressed in terms of *risk acceptance criteria.* As provided by the directive, member states can achieve this by ensuring that current levels of safety are maintained where reasonably practicable, and improved with a view to gradually harmonising safety performance across the European Community railway. The ROGS regulation which requires each transport operator to have a safety management system ensures that the mainline railway achieves its CSTs. The CSIs in the directive are categorised to address the key areas of accidents, consequences, incidents and near misses, the technical safety of infrastructure and the management of safety.

The European Commission adopted the first set of Common Safety Targets (CSTs) and the first set of National Reference Values (NRVs) for the 25 member states with railways. NRVs and CSTs are defined in terms of fatalities and weighted serious injuries (FWSI), a reporting measure adopted in the annual safety performance reports as shown in Section 2.3. The CST in each category is equal to the lower of the highest NRV value and ten times the average NRV for all member states. The CSTs cover approximately 40% of the overall risk on the railway (RSSB 2010).

Infrastructure managers (IMs) and railway undertakings (RUs) are responsible for managing their operations and are required to cooperate where they interface with other IMs or RUs, in order to deliver a safe operation. As part of compliance with regulations set out by the directive, RUs are required to have two-part safety certificates. Part 'A' is certification confirming the acceptance of the safety management system (SMS) and is issued by the member state in which the RU is based. Part 'B' is certification confirming the acceptance of the provisions adopted by the RU to meet the requirements necessary for safe operation over the relevant network. It is issued by the member state in which the RU plans to operate. IMs are required to hold a two-part safety authorisation issued by the member state where the IM is established including demonstrating an acceptance of the SMS and acceptance of the provisions to meet the requirements necessary for the safe design, maintenance and operation of the infrastructure including the traffic control and signalling system. The other noteworthy requirements are the establishment of safety authorities independent of the IMs and RUs, with the specific tasks of regulation and supervision of safety and also an independent national accident investigation body.

On this background, we establish that decisions on operational railway safety, based on risk analysis, must be against some form of criteria for risk acceptance. These criteria are used in relation to risk analysis and express the level of risk which the railway operator will accept for the activity. The term is related to the high level expressions of risk requirements and is also applicable and relevant to lower levels. Risk Acceptance Criteria used on the UK railways are usually defined at the operator level. A defined process is typically outlined for apportionment of the safety targets or goals which depend on the criteria for individual risk and whether risk has been reduced to a level which is As Low As Reasonably Practicable (ALARP).

The CENELEC (European Committee for Electro-technical Standardization) Standard 50126 provides risk assessment and acceptance principles for the European railways in line with European Railway Safety Directives presented earlier in this section. These principles include:

1. The "As Low As Reasonably Practicable" principle. ALARP is a measure of good engineering practice utilised in the railway industry in the UK and U.S is the only method described in IEC

61508. Subsequent sections of this thesis provide extensive insight into the application of the ALARP principle in the UK industry in subsequent.

2. The Minimum Endogenous Mortality (MEM) principle used in the German Railways. The MEM principle sets a global safety objective or target with reference to the endogenous mortality of an individual (i.e. the ambient risk, R_{MEM} for a person from five to fifteen years old fixed at $2x10^{-4}$ per year). A 5% contributory risk has been estimated for technical systems to the individual risk consequently resulting in a tolerated risk of 0.005 x R_{MEM}. The degree of tolerated risk becomes more stringent as the size of the population that could be affected increases.
3. The "*Globalement au moins equivalent"* principle, also known as GAME or GAMAB (Globally at least equivalent) requires that new systems fulfil the same requirements as those attained by an existing similar system. The GAMAB principle requires knowledge of safety objectives and behaviour of a reference system.

Generally, international railway safety practice employ these principles as defined in Šimić, et al (2007), Nordland (2001), HSE (2001c) and IEC 61508 (2010). These are applied to all guided transport systems.

The risk acceptance criteria that are applicable for use in the UK railway industry based on ALARP principles are usually quantitative or semi-quantitative. These criteria enable reflection on many different scenarios and the aggregation of these into one or a few characteristic values.

The basis for the formulation of risk acceptance criteria includes:

- The regulations that control safety within the activities
- The recognised norms for the activity
- Requirements for risk reducing measures
- The knowledge about accidents, incidents and their consequences
- Experience from own or similar activity

Risk acceptance criteria are subdivided in categories according to the purpose and level of detail of the analysis. The most common framework divides risks into three bands (HSE 2001c) as shown in Figure 11 and in related descriptions in this section that apply to the railway industry. Definitions of the maximum tolerable (upper) criterion and the broadly acceptable (lower) criterion for individual risk and societal risk are also presented.

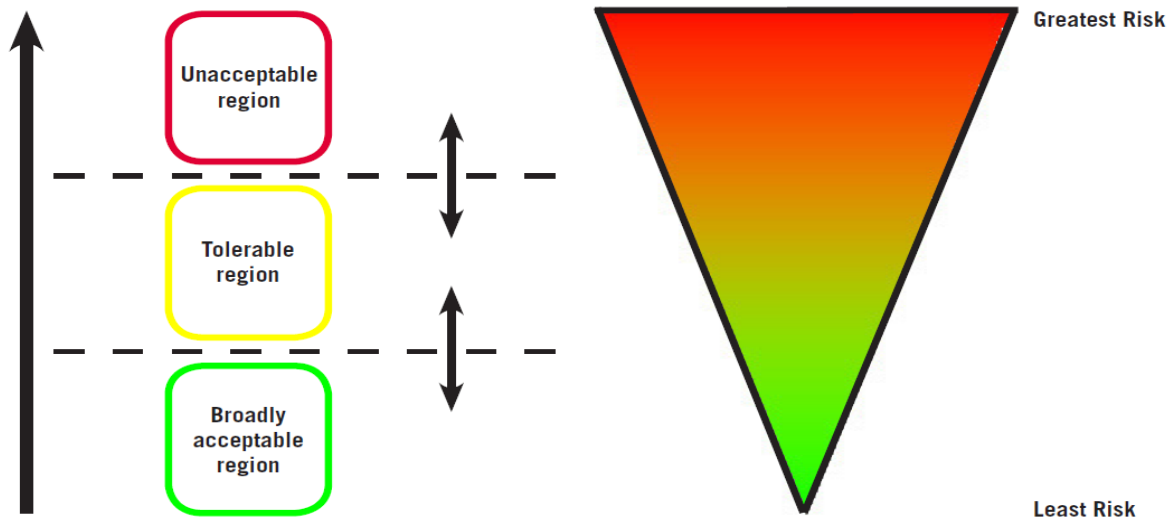


Figure 11: Tolerability of Risk Framework

The Health and Safety at Works Act 1974 and the Railways and Other Guided Transport Systems (Safety) Regulations 2006 generally provide guidance on the ALARP principle and its use as a risk acceptance criterion. The HSW Act 1974 requires that a risk assessment is completed for any undertaking. An example of this is the undertaking of a railway renewal project. If risk assessment shows that the annual risk of death is above 1 in 1,000 for workers, or 1 in 10,000 per annum for the public, then this risk is considered unacceptable. These values are representative of worker risk levels that may be observed in certain industries and of risks faced by the general public. The HSE specifies that an annual risk of death of less than 1 in one million may be classed as broadly acceptable. In setting this boundary, the HSE note that this level of risk is extremely low compared with the background level of risk that the public in general choose to be exposed to. The background level of risk is estimated at an annual risk of death of 1 in 100. Between these extremes lies the Tolerable region. Risks that fall into this category are again assessed on an ALARP basis. In providing advice on the meaning of ALARP, the HSE refer to case law which states:

a computation must be made in which the quantum of risk is placed on one scale and the sacrifice, whether in money, time or trouble, involved in the measures necessary to avert the risk is placed in the other; and that, if it be shown that there is a gross disproportion between them, the risk being insignificant in relation to the sacrifice, the person upon whom the duty is laid discharges the burden of proving that compliance was not reasonably practicable.

For effective risk assessment and risk-based decision-making, the risk for acceptance against the Tolerability of Risk framework described above is distinguished as individual or societal risk. In the HSE document, Reducing Risk Protecting People (2001c), risk characterisation is the second stage of the approach to reaching safety decisions**.** It describes this as:

The proper characterisation of the risk is important to the effective application of the preferred risk control hierarchy promoted by HSC/E and the EU. The hierarchy covers controls on hazards as well as the resulting risks. At the top of the hierarchy, and consistent with the general duty to secure health and safety, is the consideration of measures or alternatives that will avoid the hazard in the first place. This might involve substitution or the adoption of processes that conform to principles aimed at ensuring that a design is inherently safer. Lower down the hierarchy is the consideration of measures that will reduce the risks, given that there are no viable alternatives to accepting the hazard. (HSE 2001c)

(HSE 2001c) also suggests that the framing of the safety issue may point to it being one where a decision on proportionality of action requires information on the risks. In such cases, we need to characterise the risk quantitatively and qualitatively, to describe how it arises and what impact it has on those affected and society at large. Such information is needed in order to inform later consideration of options for risk reduction. Safety risk on the railways is often presented in two distinct ways, depending somewhat on the level of detail in the analysis and the objectives of the study. In most cases, specified criteria exist against which the risk characterisation option chosen will have to be compared. For effective communication of risk results, an overall view of the risk is essential. The individual risk criteria are presented in the table below, according to the 2009 safety targets.

Table 9: 2009 Individual Risk Criteria

Risk Group	Upper Limit of Tolerability (probability of fatality per year)	Annual Safety Targets (2009)	Broadly Acceptable (probability of fatality per year)
Individual passenger risk (regular traveller)	1×10^{-4} (1 in 10,000 per year)	3.75×10^{-6} (1 in 133 million passenger journeys based on 500 journeys/year)	1×10^{-6} (1 in 1,000,000 per year)
Individual employee risk	1×10^{-3} (1 in 1000 per year)	5×10^{-5} (1 in 20,000 per year)	1×10^{-6} (1 in 1,000,000 per year)
Individual member of the public risk (railway 'neighbour')	1×10^{-4} (1 in 10,000 per year)	1×10^{-6} 1 in 1,000,000 per year based on an average member of the UK population	1×10^{-6} (1 in 1,000,000 per year)

Considine (1984) defines individual risk as the risk to a person in the vicinity of a hazard. This includes the nature of the injury to the individual, the likelihood of the injury occurring, and the time period over which the injury might occur (exposure time). Widely used forms of presentation of individual risk are risk contours and individual risk profiles. Societal Risk is frequently used as it best represents risk to passengers and the wider public: it addresses the number of people who might be affected by hazardous incidents. A widely used form of societal risk is the F-N (Frequency-Number) curve, introduced previously in this section, a plot of cumulative frequency versus consequences (expressed as a number of fatalities).

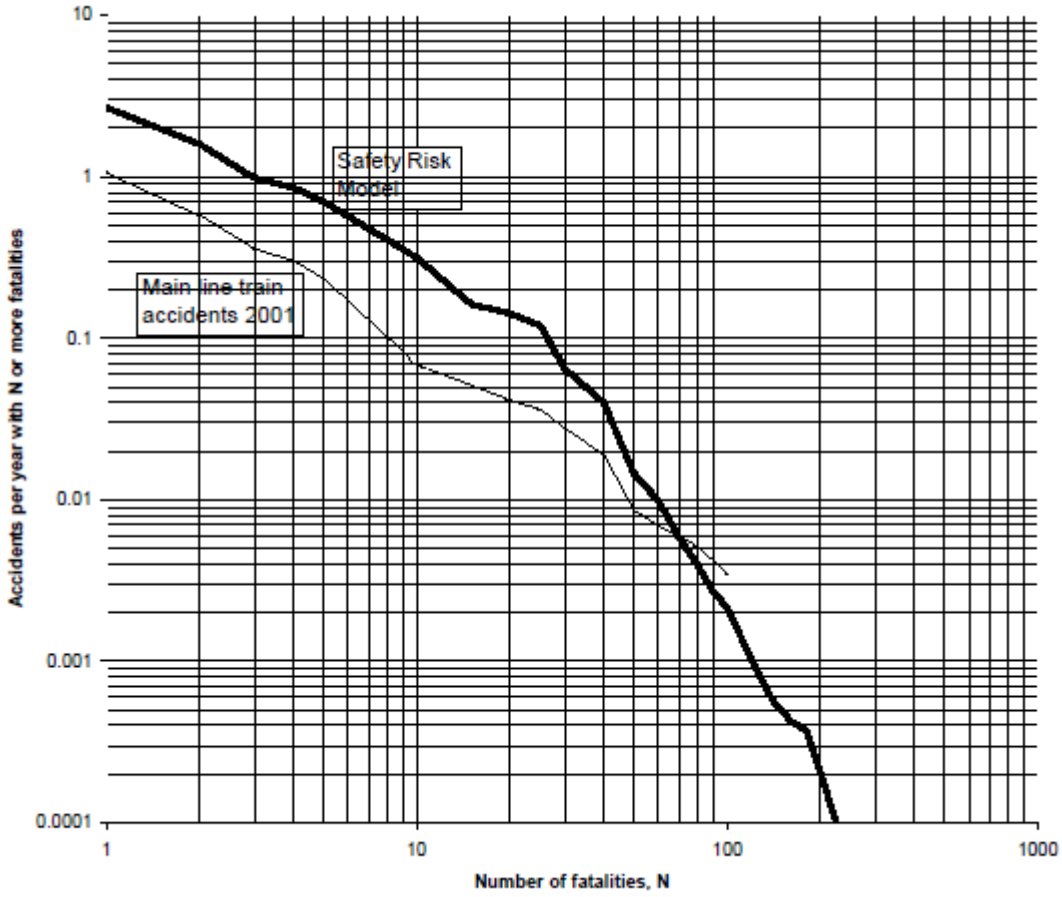


Figure 12: F-N Curve (Extracted from Evans, 2003)

This presentation of societal risks is very useful as it very clearly identifies major risk contributors. The apportionment of quantitative safety goals is usually achieved through rigorous mathematical modelling and in some cases relies on engineering judgement. A combination of the two is frequently practised. Techniques such as the risk matrix provide an alternative method for achieving the apportionment of Risk Acceptance Criteria.

Aven et al. (2006) challenge the widely held view in risk management that risk analyses cannot be conducted in a meaningful way without the use of risk assessment criteria. The authors argue that the use of such criteria is inconsistent with an efficient risk management strategy and should be replaced by a risk analysis regime that emphasizes the generation of alternatives, cost-effectiveness, and the involvement of management in the decision-making process. The study also argues that risk acceptance criteria have played a more active role in the assessment processes than ALARP. In practice, the latter is usually also carried out in a mechanistic manner, and is associated with the identification of potential improvements, however prone it may be to inaccurate use when the cost-benefit (cost-effectiveness)

analysis technique is considered for safety decision-making. This analysis is often perfunctory, or very coarse.

From a decision making point of view, satisfying the upper limit risk criteria is a different approach from an ALARP evaluation. Satisfying upper limit risk criteria is a kind of binary decision making: is this an acceptable technical solution or not? An ALARP evaluation represents a more complex situation, requiring more involvement from managers and technical/professional disciplines in order to find an optimum solution, taking economic factors, time, safety issues, and other constraints into consideration.

Kletz (2005) has suggested that by making industrial risks "ALARP risks", we inadvertently increase other risks. In other words, ALARP has served us well for many years but the time has come to move on and supplement it by considering also whether or not there is a net increase or decrease in safety. An illustration of the practical difficulty of the ALARP framework is the publicity that accidents on railways generate, which has led to politicians making promises of investment on railway safety. This leads to proposals supporting changes in line with stringent risk acceptance criteria that may not necessarily achieve the required risk reduction at a reasonable cost. However, excessive speed restrictions, extended interruptions to service, and ignorance of relative risks all drive the public on the roads, even when statistics show that highways are worse than railways in terms of safety.

Railway operations are initially associated with levels of risk that are considered intolerable based on assessments against regulatory standards or requirements where these are established. In a few countries, such as the United Kingdom, regulations include definitions of intolerable levels of risk. More commonly, internal standards of tolerability are based on the incident-related costs that an organization can bear each year, as well as the levels of risk that a given society, and its investors in particular, will tolerate. Even when the tolerability standard is met, additional risk reduction measures may be justified if the benefits outweigh the costs. Cost Benefit Analysis (CBA) often includes QRA - selected risk reduction alternatives. In these cases, internal investment criteria may be applied to select measures for implementation. A wide range of options to reduce risk is usually available. However, it takes skill to select the most cost-effective alternative. Is it better to go after a multitude of easily implemented modifications or a few options that are more effective but expensive? What to include in the overall risk must also be considered.

3.1.2 Railway Safety Risk Model

The DfT, the Office of Rail Regulation (ORR) and the industry itself have agreed that the mainline railway safety metrics will be monitored by using the SRM (RSSB 2010). The RSSB developed the Safety Risk Model (SRM), which is a comprehensive mathematical representation of more than 120 hazardous

events that could lead directly to injury or fatality on the mainline railway. The causes and consequences of each event are modelled in detail, considering the railway as a whole rather than concentrating on a particular route or operator. This provides the context for each company's management of safety, acting as a guide to the overall risk situation on the network.

The SRM has been designed to take full account both of high-frequency, low-consequence events, and low-frequency, high-consequence events. It was developed using recognised modelling techniques such as fault tree, event tree and consequence models, together with informed expert judgement. This reduces the problems that can arise with using examples from recent history which may be insufficiently representative of the underlying level of risk. The majority of the data used to populate the SRM comes from SMIS.

Taking the risk from all hazardous events together, the SRM provides estimates of the average number of fatalities and weighted injuries per year from all sources. Charts and risk estimates based on the SRM are used within the ASPR to set the context for a particular area or topic. Due to the large number of hazardous events within the SRM, ranging from minor slips, trips and falls to major collisions between trains, hazardous events of a similar type are often grouped together within the charts in the ASPR to reduce the complexity.

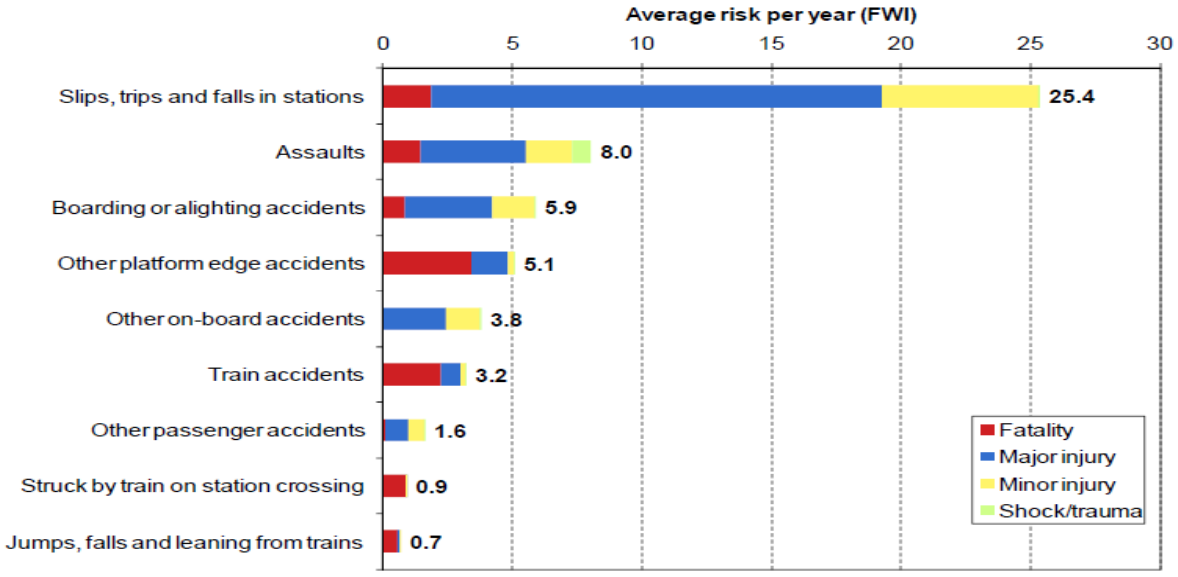


Figure 13: Sample SRM Passenger Risk Profile (Source: RSSB 2008)

Data reporting issues with the SIMS and subsequently, affecting the correctness of the SRM, are well documented in the ASPR for 2005 (RSSB 2005b). These include under-reporting, time issues, duplicates, wrong reporting and incomplete information. Under-reporting is difficult to identify and can have a significant impact. Missing records weaken the analysis and conclusions drawn may well be wrong.

Substantial under-reporting potentially leads to an underestimated risk. If the level of under-reporting changes over time, any estimates of trends may be misleading. Missing records occur because of a lack of understanding, training, guidance, or poor resources. Under-reporting is more of a concern for minor events, and the weighting that is attached to non-reportable minor injuries in part accounts for this. The consequence of late reporting is that events could be missed from an analysis. Late reporting is often down to problems with a reporting process, although most of it in SMIS is due to passengers making reports to train operators sometime after an event. An event may entered by two different organisations (or even by a single organisation twice) which can be hard to detect without manual review and can lead to an overestimation of risk. If the level of duplication changes over time, any estimates of trends will again be misleading.

Wrong reporting into the SMIS generally refers to the incorrect categorisation of events. SMIS mainly uses drop-down fields alongside a free form narrative to record event details. These types of errors can occur in any of the fields: person type, cause, or whether an event is RIDDOR-reportable. Additionally, wrong reporting can refer to a lack of sufficient information to drill down to causes. Without access to the original record, the types of checks that can be carried out are limited to checks for consistency (i.e. the coded fields tie in with the narrative description) and that different parts of the event are described consistently.

3.1.3 London Underground QRA

The London Underground Limited Quantified Risk Assessment (LUL QRA) assesses the risk of major hazards with the potential to cause fatality to customers and other members of the public. This includes risks imported to LUL operations through the activities of other LUL Group members, other train operating companies, other station operating companies and/or mainline railways. An overview of the LU Quantified Risk Assessment methods and models is provided in LUL (2012). As with the SRM, the LUL QRA excludes suicides and medical fatalities. Quantitative Risk Assessment (QRA) in general is a mathematical technique used to predict risks of accidents and to inform decisions on minimising them. The main objective of the risk assessment is to promote an understanding of the nature of these risks and provide a basis for:

- Identifying whether adequate controls are in place; and
- Identifying if any further controls are reasonably practicable

The sequence of events leading to major hazards is grouped according to their similar outcomes. These outcomes are known as ‘Top Events’ and are presented in Section 2.3.

The risk from each of model is calculated using the Fault Tree+ software tool. An Incident Capture and Analysis database (INCA) is used by LU to record incidents that occur on the London Underground Limited infrastructure. Information has been entered into this database since 1992. Incident data is entered under a particular classification, of which there are 105 different categories. The QRA models are primarily used for risk assessments and results used in the following ways:

- The QRA models provide a valuable input to the London Underground safety improvement plans and safety management, assurance activities and its results are used to inform business and planning decisions.
- The results of the LUL QRA contribute to the safety decision-making process (Cost-Benefit Analysis) but do not substitute for it
- The QRA model is used to determine the contribution of specific asset groups such as signalling or rolling stock to the total risk for a particular hazard, i.e. to support ALARP arguments. This relative risk contribution is used to demonstrate that the risk to passengers from the specific hazards under consideration is a small factor in the overall risk, and hence support an ALARP argument. This is then used in conjunction with a set of qualitative safety requirements to ensure that that the levels of risk after the upgrade shall be ALARP and no greater than the current level of risk
- The QRA models are also used to set safety targets for aspects and functions of the systems. This ensures that the risk is managed at a level no worse than the current state, making the results useful as a baseline for engineering renewal projects. The model provides a valuable base-line measurement of current safety standards against which any proposed change to equipment, procedure, organisation or any other aspect of operation can be judged in terms of its effect on safety.

It may be argued that QRA applied in the Railway industry as a decision support tool is somewhat unsophisticated as it has been simplified somewhat with readily available easy-to-use tools for risk quantification. There has been a tendency for QRA to be treated as an isolated analytical exercise, with only a loose link to other risk management activities, despite the use of QRA for risk measurement and as part of risk assessment process to meet industry, regulatory and in some cases cost targets. On the other hand, some engineering safety professionals may argue that QRA can be regarded as a key method of 'scientifically' attempting to characterise the uncertainty that surrounds hazard and exposure assessment processes. Notwithstanding the 'scientific' tag attached to QRA, some regard it as an immature and highly judgemental technique, with results that have a substantial degree of uncertainty (Spouge, 1999).

The RiskVu and Fault Tree+ tools have been developed to assist in estimating the safety impact of any change affecting the LUL QRA. The estimation of risk for a particular Top Event is achieved by the evaluation of the likelihood and the consequences of the hazardous event under consideration.

To determine the likelihood of the Top Event occurring, the contributory causes of each of the major hazards are identified and the frequency or probability of the event is determined. The latter is determined through fault tree analysis. The consequences of a hazard are defined in terms of the theoretical number of deaths arising.

This severity and the probability of occurrence of the Top Event are combined (using event tree analysis) to determine the risk associated with each Top Event. This is summed to determine the total risk for each of the Operating lines, each Business Unit and the LUL network.

The level of risk is expressed as fatalities per year. This figure is the aggregate of a number of possible consequence outcomes for a given Top Event. It takes into consideration the possibility that realisation of a hazardous event does not always result in the worst case consequences but may have a number of different outcomes, including in some circumstances no fatalities. It also takes into consideration the probability that an incident may occur at any time. Thus the risk estimated by the LUL QRA is the aggregate of these possible frequency and consequence outcomes.

The actual number of consequences in terms of fatalities used in the LUL QRA model are derived from a combination of historical incident data, consequence analyses (where available) and expert judgement. The results of the LUL QRA are presented in the form of a 'Risk Profile', a 'Summary Table' and, for the LUL Network only, an 'F-N Curve'. A Risk Profile [Figure 13] is a graphical representation of the risk attributed to each Top Event. It allows these dominant major hazards to be easily determined. Line Risk Profiles are produced for each of the LUL Operating lines, for each Business Unit, and for the LUL Network. Summary tables provide a breakdown of the risk for each Top Event and typically used to support the risk profiles. The major hazards are listed in order of dominance, with the percentage contribution of the Top Event to the overall LUL Network risk also shown. The main scenarios which make up each Top Event are also listed in order of dominance with their percentage contribution to the Top Event indicated. F-N Curves and presentations of risk profiles using F-N Curves are discussed in Section 3.1.

The use of fault trees and similar techniques for risk analysis which inform risk-based decisions come with disadvantages which may be catastrophic. Their use in a high hazard industry such as the railway network should be supported by thorough assessment and validation. The report by Turner et al. (2002) highlighted some weaknesses in the software tools used to build event and fault trees.

- Large event trees cannot be scrolled around and are therefore difficult to read, with a potential to introduce errors into the models;
- Fault Tree+ allows the use of partial event failure nodes in the event trees. This gives the analyst flexibility although it does not check that the sum of the partial event probabilities for a specific sequence is equal to 1.
- Not all identified contributing events to the accidents are included in the fault tree models in order to manage the level of detail required for analysis. In so doing, only high-level contributing events are included because of limited data on the root causes of some failures. The concern here is that the methods employed for deciding whether particular identified contributing events should have been included into the fault tree models or not are usually very subjective and without structure or logic. This opens a debate on the likelihood that the results for the railway operation quantified risk assessments omit some scenarios in which a particular hazardous event may occur.

However, Turner et al. (2002) found that the errors are minimised because the risk models were constructed at a relatively high level. The SRM does not model the root causes of failures. Models of significant size and complexity similar to the SRM are not expected to be totally error free.

Where data was available, detailed models with identified contributing events were incorporated into the risk models. These acknowledged modelling limitations indicate that the risk models can only support safety decisions at a relatively high level. The findings also indicate that no modelling of controls was undertaken in the risk models, so that it was difficult to predict the link between the contributing events, controls and the safety management system.

The basic events that are quantified as frequencies (events per mile) are modelled in the fault trees as probabilities. This is inaccurate because when a fault tree is quantified, these frequencies are multiplied together (cross-product terms) resulting in an inaccurate probability of the Top Event. Quantification of many of the events in the high consequence/low frequency classification such as train accidents are based on very few past incidents, sometimes as low as only one or two. This supports the case presented in Turner et al. (2002) that high consequence, low frequency accidents are underrepresented in the SRM.

With the limited data available, particularly for high consequence/ low frequency type train accidents and even where this data exists, the quality becomes an issue. Consequence data used in the risk models are therefore subject to great uncertainty. Most analysts will quickly express concern about the lack of historical data available for a comprehensive analysis. These methods of risk analyses are viewed as

flawed because they depend heavily on incorrect data (Weli and Todinov, 2013a). Other factors that influence the accuracy of the data are the experience of the analyst and expert opinion/judgement for estimating event frequency and consequence.

3.1.4 Human Error Assessments

In general, human error estimates are deduced from human reliability techniques such as the Human Error Assessment and Reduction Technique (HEART). These remain questionable. Human error related events are modelled as contributing events in fault trees and consequence models. In the SRM, HEART or expert judgement are used to produce estimates of human error probabilities. HEART was not developed specifically for the railway industry; Kirwan (1994) points out that this technique fails to consider crucial factors such as dependence. The SRM considers major and minor injuries and is therefore quantified in terms of equivalent fatalities. However, the findings indicated a small concern that there was no clarity on the rationale for the ratios used to convert a major and a minor injury into an equivalent fatality. This is an industry-wide concern as this technique was in use before the SRM and to date; no strong argument has been put forward for the ratios. The findings show that a considerable analytical effort needs to be applied to understanding the role of uncertainty in developing the SRM, leading to the conclusion that the SRM is largely based on pessimistic judgements.

For decision making on delicate issues such as the safety of persons / passengers on UK railways that may potentially have adverse effects on the safety and risk sensitivity of the society, a company's adopted risk management process must also address an ethical and value-driven commitment to risk reduction. HMRI (2006) requires that intolerable risks on the railway be eliminated and all remaining risks to be reduced to as low a level as reasonably practicable (ALARP). HSE (1999) further requires that 'suitable and sufficient' risk assessments be undertaken. This often leads to the question - does a qualitative risk assessment meet legislative requirements taking into account the uncertainty associated with quantitative risk assessment? Are we sufficiently meeting legislative requirements by using both?

In view of the broad scope of the risk models used for decision making and safety planning and despite the weaknesses highlighted, the risk models do meet the high-level objectives of analysing and presenting quantified safety risks on the UK railways. The improvements to be made will be capital and time intensive. In a statement clarifying the effort put into these models, the board known as Railway Safety (now the Railway Safety and Standards Board) stated and quoted in the Health and Safety Laboratory's Review of Railway Safety's Safety Risk Model by Turner et al. (2002) that 'many person months of effort were expended in resolving the fault trees as far as possible but were ultimately limited by the availability of suitable data. And indeed, the collision models do include some 500 individual cause precursors.'

The two main railway operators with responsibilities to the Organisation for Rail Regulation (ORR) for applying a robust Safety Management System and meeting specifications in Railway Operators' Safety Cases extensively use these methods to support their case for safe operations. Considering the above and the extensive use of QRA as a risk assessment tool on these two major railway operators in the UK, it is worthwhile evaluating further the practice and application of QRA and risk assessment on UK railways.

3.2 Impact of Accidents on the Existing Risk Assessment and Risk Management Strategy

The major accidents discussed in Section 2.5 highlighted that the most critical challenge faced in achieving rational risk reduction through existing railway safety risk assessment and management strategy has been the decision-making process. This subsequently resulted in:

- Significant changes in operational procedures;
- Introduction of onerous requirements for introducing systems into the operational railways and subsequently;
- Encouraging specific amendments to the techniques for risk assessment and management.

One such vital amendment was the replacement of three key railway safety regulations, the Railways (Safety Case) Regulations 2000; Railways (Safety Critical work) Regulations 1994; and the Railways and Other Transport Systems (Approval of Works, Plant and Equipment) Regulations 1994 with the Railway and Other Guided Transport Systems (Safety) Regulations 2013 (ORR, 2013).

These three major regulations set the baseline for all risk assessment and management strategies to be adopted by railway operators, infrastructure controllers, station operating companies and infrastructure maintenance contractors. The Railway (Safety Case) Regulations 2000 was introduced to ensure that safety is established and managed as an inherent part of the operation of trains and set out well defined requirements for developing and maintaining a Railway Safety Case (RSC). Under this strategy, the railway safety case was assessed and accepted by the HSE giving confidence that the operator has the ability, commitment and resources to effectively assess and manage the potential risks to the health and safety of staff, contractors, passengers and the public. The railway safety case should clearly define:

- The nature and extent of the operations to be undertaken;
- The safety risk associated with these operations;
- The procedures and arrangements by which the risk is controlled;
- The organisation in place for implementing these procedures and arrangements;

Guidance notes and standards within the railway all adopted the RSC 2000 regulations but in line with new regulations were withdrawn. It is worth noting however, that despite the new regime of regulations,

the industry-wide risk assessment techniques have generally remained unchanged, because risk assessments to support railway operations are still subject to the Health and Safety at Work etc. Acts 1974, and the Management of Health and Safety at Work Regulations 1999, from which the requirements to undertake risk assessments originated.

The Railways and Other Guided Transport Systems (Safety) Regulations, herein referred to as ROGS, was introduced to put the requirements of the 2004 European Railway Safety Directive into practice. The directive aims to continue to remove barriers to providing international transport services by creating a common framework for railway safety across the European Union. This sits alongside the European Interoperability Directive, which aims to remove the technical problems involved in running trains between member states. ROGS puts in place some of the main requirements of the safety directive in Great Britain.

The main objectives of the Railway and Other Guided Transport Systems (Safety) (Amendment) Regulations, 2013 are to:

- Change the industry's system of railway safety cases to a system of safety certification and authorisation and ensuring that Common Safety Targets are understood and met;
- Produce a minimum set of requirements for a Safety Management System so that safety certification is simplistic without having to get through layers of government or authorising bodies;
- Ensure that transport operators and infrastructure managers work together to provide required system safety;
- Redirect inspection towards checking to ensure that operators are managing their operational risks;
- [Operators to] Institute adequate cooperation methods that complement the measures they are taking to comply with their own safety duties – interface risk management;
- Replace the approval of new or altered works, plant or equipment with safety verification from an independent competent person (ICP);
- [Ensure that] competency management and safety-critical work is undertaken by a person assessed as being fit, change the system of controlling hours for preventing fatigue to the control of risks resulting from pattern of working hours and roster design.

The ORR commissioned an evaluation into the effectiveness of ROGS presented in ORR (2010). The evaluation methodology was based on establishing the ultimate and subsidiary objectives of ROGS as outlined in this section and on collecting a range of evidence over a three-year period using industry data

from duty holders and non-duty holders to help assess whether or not the Regulations had achieved their intended objectives. This addressed the most important parts of ROGS such as Safety Management Systems, Safety Verification, Safety Certification, Safety Authorisation, Risk Assessment, the Annual Safety Report, Duty of Cooperation and Safety-Critical Work that significantly influence existing railway industry risk assessment and risk management strategy. The industry survey indicated the following key findings:

1. In terms of awareness and understanding of ROGS, the survey showed that 57% of the respondents to the survey required guidance in understanding and implementing ROGS.

2. Most respondents did not understand ROGS near-miss reporting and lacked adequate understanding of work-related risk.

3. Perceptions of management getting staff involved in safety-related decision-making and safety being a key priority was positive.

4. A considerable percentage, 35%, agreed that they are placed under pressure to meet operational performance objectives and that such pressure affected safety.

5. A majority of respondents confirmed that ROGS had changed the way that safety is managed, while 43% felt that safety-related decision-making had been influenced by ROGS. However, a majority agreed that standards of safety are the same under ROGS.

6. About 83% of duty holders reported having a Safety Management System (SMS) in place.

7. Over half of the respondents stated that the cost of maintaining a SMS is similar to the cost of a safety case.

8. It was found that the most common challenge of maintaining a SMS was ‘communicating the SMS to the organisation’.

9. In terms of introducing new / altered infrastructure or rolling stock, the majority of duty holders had either SMS change management process or safety verification under ROGS. However, identifying and appointing an ICP and knowing when to apply safety verification were the most common challenges cited by the respondents. The majority of the responses indicated that safety has not changed because of safety verification.

10. There has been an increase in the number of respondents who reported that their organisation had completed each stage of the safety certification process and that less time is spent in the

ROGS certification process against Railway Safety Case applications. Comparing the cost of ROGS safety certification against Railway Safety Case applications, the majority of respondents confirmed that the costs were less under the former. The majority of final year respondents indicated that there had been 'no change' to safety due to safety certification under ROGS. The majority of the respondents confirmed that it takes less time to undertake safety authorisation applications than Railway Safety Case applications. However, the most common challenge reported by the final year respondents in acquiring safety authorisation was 'understanding the requirements' and that 'safety authorisation had not affected safety'.

11. Many respondents indicated that there have been no challenges encountered in adapting existing risk assessment arrangements to meet the requirements of Regulation 19. The majority of respondents (88%) indicated that there had been no change to safety as a result of changes to risk assessment.

12. The majority of respondents felt there had been no change to safety as a result of the introduction of the duty of co-operation.

13. Encouragingly, when asked about the challenges encountered in meeting the safety critical work duty, the most common response was 'no challenges'. Apart from this, 'training staff and managers' and 'understanding the requirements' were the most commonly cited challenges.

14. 88% of respondents indicated that there had been no change in safety as a result of the safety critical work duty.

These findings, mapped against each one of the ROGS objectives for improving safety on the railways through amendments to the existing risk assessment and management framework indicate that ROGS had either achieved the original objectives or progress has been made in achieving them. The findings also indicate that the introduction of ROGS had not increased the financial burden to the industry and in some cases had actually been more cost effective than the previous strategy. However, when the question was posed on safety improvements since the introduction of ROGS, the general view of duty holders was that ROGS had not brought any changes. This is the underlying criticism of ROGS, a conflict of cost against safety improvement leading to the question: Has ROGS really been beneficial? The difficulty in deciding whether the ROGS strategy is enough or requires substantial overhaul in terms of the key elements of ROGS (i.e. Safety Management System, Safety Certification, Safety Verification, Safety Authorisation, Risk Assessment, Annual Safety Reports, the Duty of Cooperation and Safety Critical Work Duty) has recently led to the Railway and Other Guided Transport Systems (Safety) (Amendment) Regulations 2013 (ROGS).

3.3 Existing Risk Assessment and Risk Management in the Operational Railway

Risk assessment leading up to safety benefit analysis in high-level decision-making terms is largely driven by concern with health hazards. For the public, it is the key assessment of risks associated with the operation of a railway network. The Management of Health and Safety at Works Regulations 1999 makes reference to the need for risk assessment to be 'suitable and sufficient' depending on the nature of the undertaking and the type and extent of the hazardous events and other factors that exist. The definition of 'suitable and sufficient' has historically been difficult to establish due to the broad application of risk assessments and of the operations requiring them. The process for risk assessment has been widely studied and documented. A thorough review of withdrawn and existing internal railway industry guidance notes and standards has ensured that the appropriate level of risk assessment is performed for any railway, as shown in Figure 14 below.

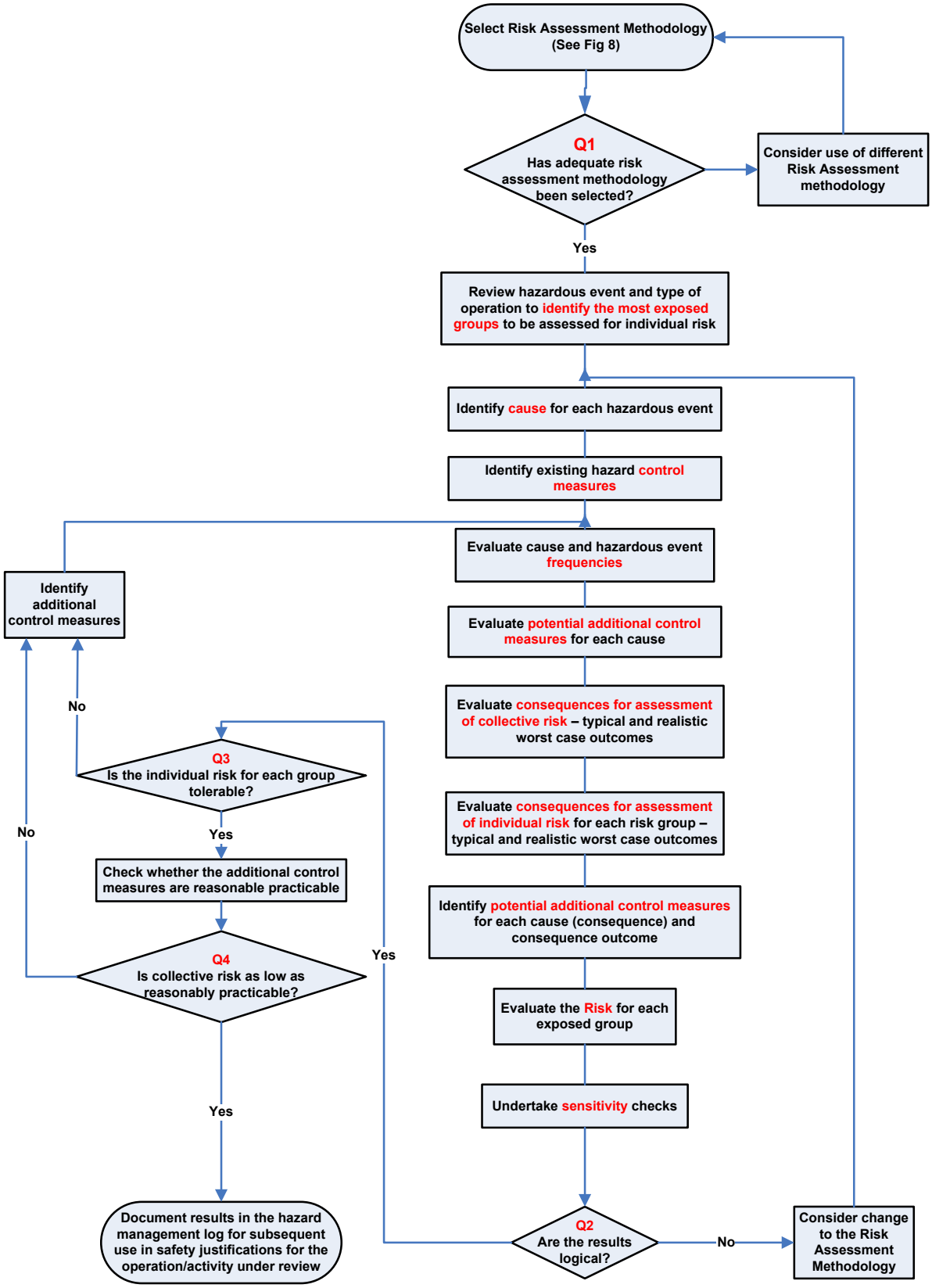


Figure 14: Generic Risk Assessment Methodology

Steven G. Gilbert suggests a 4-step process for risk assessment in his paper 'The Precautionary Assessment: Getting out of the Risk Assessment Box' (November 2006). Borysiewicz et al.'s report on Quantified Risk Assessment for the Institute of Atomic Energy (2004) outlines relevant steps in the major accidents risk assessment process. The Yellow Book (RSSB, 2007b) published by the UK Rail Safety and Standard Board, which sets out the fundamentals of Engineering Safety Management on the railways, also provides guidance, defining a 7-stage process for risk assessment. In a similar pattern, other risk assessment books and articles from specialists in different industries, including Chemical, Medical, Energy, Transport and Construction sectors have outlined steps for complete risk assessment, as summarised below:

1 Hazard Identification;

2 Estimation of the frequency and consequence of accidents. The Yellow Book further breaks this down into Causal, Consequence and Loss Analysis. Estimation of the consequences of each possible event often requires some form of computer modelling but in some cases is based on accident experience or judgements if appropriate;

3 Risk Characterisation following modelling could involve the presentation of risk in various forms. The representation of risk to life takes two different forms:

- Individual Risk – the risk expressed by one person exposed to the hazard
- Societal or Group Risk – the risk experienced by the whole group of people exposed to the hazard being analysed.

Hazard identification is the first and most important step employed if the overall risk is to be adequately analysed. It involves the identification of all relevant hazards and initiating events applicable to the system under review. Identified hazards will then be assessed to extract events which may potentially lead to the main hazard or an accident on the operational railway (LU Top Event or SRM Hazards). A preliminary estimation of the likelihood of identified events which may potentially lead to an accident is then undertaken.

The Yellow book as a fundamental guide for Engineering Safety Management on the Railways makes a simple statement on hazard identification: '*Your organisation must make a systematic and vigorous attempt to identify all possible hazards related to its activities and responsibilities*.' There is no rigid or sequential technique stipulated for hazard identification. Several guidelines and techniques exist and these can be used in various combinations to improve hazard identification.

The reasons for systematic and complete hazard identification at the onset of all risk assessment processes are

- To Identify system hazards at the concept and feasibility stages of a system design or operation that flow back into design or operation, allowing early implementation of design or operational changes;
- Support comprehensive and acceptable risk estimation and quantification;
- Facilitate the generation of appropriate mitigation measures, actions and safety requirements.

One key relevance of the hazard identification process as part of the wider quantified risk assessment, referred to earlier is the 'classification and selection of initiating events'. An understanding of these initiating events through existing data and past experience can assist in simplifying the overall quantification of risk.

Confidence in the degree of accuracy and uncertainty of accident/hazard frequency estimation (which are part of the risk assessment process utilised in fault tree analysis, event tree analysis and consequence modelling in both the LU QRA and SRM, as presented in Section 3.1.) is the subject of many deliberations amongst safety risk professionals. The loopholes in estimation techniques currently in use, and their possible future developments are presented in this section.

Event probability estimation can be derived from two distinct but related resources:

- Historical data
- Analytical techniques

The historical data method involves the use of statistical data or empirical data from existing system or similar systems. This method is often used on railways where massive collections of empirical data already exist. A .W. Evans (2003) used data from as far back as 1967. Where there is significant and trustworthy empirical data, the analysis tends to be straightforward. Such data often include all contributors to the accident under review, with other factors such as

1. System reliability
2. Operational processes
3. Quality Assurance
4. Human Factors

5. Environment

6. Maintenance / Maintainability

In cases where the historical data is inadequate, a combination of sub-events is used and the predicted event probability is tested against existing data. This determines whether the combined sub-events and existing data are comparable. Basic errors made when using historical data, which are often ignored during risk analysis, are:

- Over-estimation caused by inclusion of contributory factors not necessarily applicable to the analysis;
- Empirical data from old systems which may not apply to the newer systems with improved standards.

The analytical technique is adopted where the historical data is inadequate, unavailable, or the system failure/accident probability is different from that indicated by the historical data. The analytical technique uses either a logic top-down or bottom-up approach by breaking a Top Event or accident down into its contributory sub-events or causes. These sub-events, with failure or accident data will then be combined through mathematical functions, built into the models, leading to a resultant Top Event or accident.

The analytical techniques employed by the safety expert or risk analyst in the railway industry rely on logical combinations or a sequence of events which ultimately lead to an accident, or Top Event. When a bottom-up and top-down combination is used in the analysis, omissions are easily detected and corrected.

Where the sub-events have no related data, expert opinion on accident frequency estimation is sought. In cases where expert opinion has been employed, usually during quantified risk assessment workshops or sessions, tree logic and data evaluation are brought in. The use of expert opinion, despite being the only alternative at this stage, results in a degree of scepticism about the accuracy of the results.

The breakdown of events into sub-events aims to improve judgement on the likelihood of an event. The event is sub-divided into smaller units for easier estimation. This is achieved by a further enquiry of the participating experts. It is then assumed with some degree of confidence that the overall outcome is less sensitive to any one particular judgement or input from an expert. However, this technique has some crucial disadvantages:

- ***Inappropriate interchanging and combination of frequency and probability in the analysis*** – this is down to the expert analyst although adequate review of the models can easily identify these types of errors for smaller models. Becomes extremely difficult for larger models. as a single change can introduce an alteration of the entire work;

- ***Rationality of the experts providing estimates*** – the rather optimistic assumption that the individuals or expert undertaking the analysis will choose the best options (events, combinations, logic etc.) leading to the Top event or accident;

- ***Availability bias*** – a phenomenon which may result in cognitive bias in which people predict the frequency of an event based on how easily an event can be remembered;

- ***Quantified consequences are mostly pessimistic*** as a result of the consideration of conservative assumptions made in each part of the logic chain of consequence analysis.

The neglect of human factors may also affect the level of uncertainty in the analysis especially when analytical techniques such as fault tree analysis are used for estimation. Experience indicates that a good percentage of system failures or accidents are usually linked to human error (i.e. installation, maintenance, operational errors). There is usually a great degree of assumption (at what level we can only imagine) that compromises the quality of assessments for human factors.

The level of confidence in the deficiencies of these models and their use is further compounded by the measure of accuracy of a probability estimate based on data. Inaccurate data can lead to a misleading failure rate, resulting in inaccurate estimation of the accident probability. Questions arising when determining the level of accuracy of a quantified risk assessment may include but are not limited to:

- Have all sub-events been included in the risk models?

- Can we trust the data and the source?

- Have all failure modes been identified and their criticality and combination adequately checked? It is easier to identify and evaluate single failures using qualitative means, but combining the sets contributing to a Top Event or accident requires in-depth reviews, often from different reviewer(s).

- Is the accident an extremely rare event? Rare events usually have a higher degree of uncertainty as it is difficult to deduce accident frequencies or probabilities and hence the need for heavy reliance on expert judgement.

In a review of system reliability estimates, Lees and Frank (1996) showed that estimates of system reliability were fairly accurate. In a study of 130 diverse systems and equipment, 63% of the predictions were within a factor of 2 of the observations and 93% were within a factor of 4. However, Weli and Todinov (2013a) have illustrated the inadequacies of accident data estimates specifically in railway risk reduction applications.

Chapter 4 Economics of Safety and Safety Budgets

There is very limited published material on the economics of safety and safety budgets that directly applies to the railways. Extensive research is undertaken into the economics of safety from the government, regulatory bodies and operators that play a key role in the allocation of funds based on risk targets for the railways. This section also demonstrates the link between the government, railway operators or sub-contractors in the application of safety economics, its impact on the public, and its overall effect on the operation of the railways.

Extensive work to support a framework development in the field of safety economics and safety investment decisions has been undertaken by Arrow and Lind (1970), Jones-Lee and Loomes (1995), D. Currie (2000), Veltri and Ramsay (2009), Fischoff et al. (1981), and Todinov (2001). The findings of other notable scholars in economics with work directly related to safety are also carefully studied and presented here. These studies were useful references and very extensive, but they do not address the issue of optimising risk reduction measures. However, they lay the foundation for developing the framework for achieving maximum risk reduction with budget constraints. The operational rail network, in the opinion of the author, needs this fundamental study to ensure railway safety improvement and considerably reduce the costs which invariably leads to increase in customer benefit.

With the objective of maximising risk reduction, this chapter considers in depth, how decisions to support optimisation of risk reduction with budget allocations are made by providing a general yet thorough overview of the application of basic economic concepts in railway safety. This includes the application of Cost Benefit Analysis. The chapter concludes that the current limitations of applying these concepts to engineering safety risk reduction are mainly due to lack of understanding of application objectives and poor link between the different phases of the engineering lifecycle i.e. concept to decommissioning.

4.1 Economics of Safety

Excerpts from a Department for Transport publication on the **Cost of Railway Incidents** entitled 'Proposed Amendments to the Railways (Safety Case) Regulations 2000 Regulatory Impact Assessment (Post Consultation)', *provisionally* estimate that the total annual losses from railway incidents (of all types) is £120 million each year at current price. At the time of developing this thesis, the research was not yet finalised, and may be subject to change. The figure of £120 million should be taken as a good central estimate although it is subject to uncertainty in the data. The estimate includes all the losses associated with accidents, including valuations for fatalities and injuries, which follow the DfT's valuation of fatality prevention (based on the willingness to pay among a wide group to avoid a small increase in

personal risk, equivalent to one fatality amongst the whole group). The cost of public inquiries that may arise from major incidents is not included.

A study of the accuracy of cost estimates in transportation infrastructure planning found that for rail projects, actual costs turned out to be on average 44.7 percent higher than estimated costs, and for roads 20.4 percent higher (Flyvbjerg, Holm, and Buhl, 2002).

These costs or losses (in some cases, very significant) provide the case for the industry's urgent requirement of robust risk reduction techniques for prioritising and optimising safety investments across all operational railway systems. This would effectively develop the means of adequately assessing safety return on investment and, through the adoption of risk tolerability thresholds and the value of preventing fatality criteria.

In most safety critical projects (including the railways), decisions on future projects are made based on answers to questions such as:

- Will the investments on safety contribute to economic performance – short and long term?
- How much do we invest considering budget limitations?
- What products / services do we invest in to maximise safety and economic benefit?

The management of current railway operations management takes the view that safety investments are costs to be controlled primarily because of regulatory constraints. Nave & Veltri (2004) and Veltri, et al. (2003a,b), point to the need for traditional approaches to justify safety investments in order to yield a new and more economical way of thinking. Applied to this study, this means the development of a framework, techniques, tools and practices that wholly consider the necessary facets of regulations, technology and commerce to achieve efficiency. In a world where finance and the availability of funds are crucial, making a business case for the introduction of safety measures and methods within a fixed budget will require a methodology that optimises the investment on risk reduction, ultimately helping the duty holder to understand where the greatest operational risks lie, what accurate risk reduction measures to apply, what precise budget requirements are needed and what is the expected benefit.

The application of optimum risk reduction techniques, tools and practices supports the railway safety case and safety management systems. This further assists the duty holder in the process of demonstrating safety adequacy to the safety regulator.

Currently, CBA is the methodology employed when considering benefits of introducing risk reduction measures. Although it is relatively easy and simple to apply, there are many arguments against its use

because of the potential for inaccurate results. On safety-critical systems or industries such as the railways, oil and gas, nuclear, utilities, medical etc., wrong decisions based on CBA may be catastrophic. These are a result of the high level of errors introduced and the uncertainty posed by this method. There is therefore an urgent need to develop a new framework.

The Railway Safety and Standards Board, as part of their Safety Decisions Programme documented in RSSB (2007), present a common understanding amongst railway industry stakeholders as to what the railway is expected to deliver with regard to safety. Some vital extracts from this document are presented below.

The legal duties that rail companies must discharge in the UK when taking decisions that affect safety are based on a complex mixture of case and statute law. In particular, sections 2, 3 and 4 of the Health and Safety at Work Act 1974 (HSWA) require all employers, including railway companies, to reduce risk so far as is reasonably practicable (SFAIRP). There is the potential for conflicting views about how to interpret the law. However, key rulings (one of which is presented in this section) help clarify how the railways can determine what measures are reasonably practicable. Ultimately, each decision taker is responsible for assessing if the proposed course of action is reasonable and if necessary, has to defend that decision in court. The duty holder(s) must satisfy themselves that a particular safety measure is reasonably practicable. If a decision were ever to be questioned in court, a magistrate or jury would apply the reasonable practicability test.

A key case that clarifies a company's legal duty is Edwards v. the National Coal Board [1949] 1 All ER 743. The ruling in this case states that:

… a computation must be made in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them - the risk being insignificant in relation to the sacrifice - the defendants discharge the onus on them.

In defining the factor or algorithm for what constitutes grossness, the Health and Safety Executive states in HSE (1988) Tolerability of Risk from Nuclear Power Stations (TOR) that:

Precise values for this multiplier have never been defined by the courts and neither the regulator nor the regulated have sought this; both recognise the drawbacks associated with trying to regulate by means of (arbitrary) numbers…

When safety improvements are being considered and the cost is less than the monetary value of the safety benefit determined by applying the VPF, duty holders generally implement the improvement.

Where the cost is above the monetary value of the safety benefit, professional judgement is applied in determining whether the cost is grossly disproportionate to the safety benefit and it is reasonably practicable to implement the improvement. In making this judgement, particular attention is paid to:

- The degree of uncertainty in the assessment of costs and safety benefits
- The range of potential safety consequences.

For a quantitative analysis, the CBA approach is to compare the cost per statistical fatality avoided (CPF) with the value of preventing a fatality (VPF). If the cost is less than the monetary value of the safety benefit determined by applying the VPF, we generally implement the improvement. Where the cost is above the monetary value of the safety benefit, we apply professional judgement in determining whether the cost is grossly disproportionate to the safety benefit and whether it is reasonably practicable to implement the improvement. The VPF is derived from Willingness to Pay (WTP) studies involving members of the public.

The VPF is usually defined as the amount that the average member of the general public is willing to pay to reduce the average level of risk to the average victim. This may be estimated by asking a representative sample of the public how much they would be willing to pay to reduce the probability of various low-frequency harmful events, then weighting this finding to calculate the amount that should be spent to avoid one statistical fatality. In principle, it is a robust and logical definition, and, because it uses people's opinions on situations that might affect them or others, it is a direct measure of societal values.

There is broad consensus in the industry that risk assessment is an uncertain process, and that this uncertainty must be taken into account when making a judgement about the relative balance to be struck between costs and risks. This view is also reflected in the HSE (2001), which states that:

The quality of the modelling and the data will affect the robustness of the numerical estimate, and the uncertainties in it must always be borne in mind when using the estimate in risk management decisions. The use of numerical estimates of risk by themselves can, for several reasons including those above, be misleading and lead to decisions which do not meet adequate levels of safety. In general, qualitative learning and numerical risk estimates from QRA should be combined with other information from engineering and operational analyses in making an overall decision.

The Health and Safety at Work Act (1974) stipulates that expenditure to reduce hazards must be incurred up to the point where the remaining risk is 'as low as reasonably practicable (ALARP)'. The 'Safety Justification and ALARP' standard describes the approach to demonstrating ALARP, and the method and parameters to be used when assessing the value of safety benefits.

Expenditure on safety to minimise the occurrence of incidents, which could lead to loss of life, injury, or damage to assets is expressed in financial terms. In order to compare the magnitude of the safety benefits with the expenditure and arrive at an estimate of whether or not the expenditure is worthwhile, the benefits must also be expressed in financial terms. On the railways, a simple approach is utilised for project cost valuations. If the probable frequency (expressed as the number per annum) of an event occurring and the probable impact if the event occurred (expressed financially) are known, then the product of these two numbers is the expected cost per annum of the risk. If as a result of the expenditure the magnitude of either or both of these two quantities is reduced, then the reduction in annual costs can be ascertained and used in appraisal calculations in the same manner as any other benefit. The allocation of funds and resources to safety then raises a topical debate on the interface between safety and commercial aims on any project or programme.

Following extensive research on railway organisations' internal practices, it became clear that in today's railway safety two methods are used to integrate safety and commercial objectives on a project:

- The Cost Benefit Analysis approach
- The Target Setting Approach

The two methods are standard ways that facilitate decisions on project safety investments on the railways and will be discussed in further detail later in this chapter. Although these are useful methods in analysing investment decisions, their exclusive use can result in incorrect decisions such as accepting project proposals that lose money or rejecting proposals that may represent financial opportunities. One of such CBA-based methods or tools is the SH&E Economic Analysis Model proposed by Veltri & Ramsay (2009). The model is an abridged CBA analysis with similar inherent limitations (discussed further in Section 4.2). The foundation of the proposed condensed model as presented in Veltri & Ramsay (2009), is based on the unabridged framework developed by the Society of Environmental Toxicology and Chemistry. The objective of the model is to help answer questions on organisational Safety Health and Environmental investment allocation. These include:

- Which products, technologies, processes and services tend to drive SH&E life cycle cost?
- Which SH&E management strategies and technical tactics should be pursued and what level of investment will be required?
- What is the potential business contribution over the short and long term?

Present value financial analysis is used in this case to provide a means of:

- Comparing the financial performance of mutually exclusive alternatives;

- Delineating the long-term financial impact of SH&E investments by presenting the after-tax cash flow and the present-cost value of the investment over a sufficient time horizon.

The rationale for using net present value financial analysis is that many of the traditional financial analysis techniques employed by SH&E specialists, such as payback and rate of return on investment, fail to take the time value of money into consideration.

The business case development manuals used by railway operators set guidelines on presenting a safety business case based on CBA. Proposals for change or implementation of a new system, product or resources must be presented with a Business Case. The business case enables authorising bodies or personnel to make informed decisions for change or system introduction including risk reduction measures for sustainability, profitability and best use of limited funds. A basic checklist is outlined in the manuals that satisfy the subject of 'Is this cost necessary?'

- Compulsion – statutory requirement
- Cost effectiveness
- Risk avoidance
- Risk tolerance – removal or reduction
- Profitability and Sustainability
- Miscellaneous expenditure – what we might call running costs

As outlined in the manuals, appraisals on a business case is undertaken to identify the impact that an action will have on the finances of an organisation and in achieving efficiency, economy and safe operation of the railway. Essentially, a base case is presented as one of the options and other options will be to implement a change with expected returns. The options provided should be able to show that the implementation of the change or introduction of a new measure will bring total benefits that surpass the cost of implementation. The appraisal will need to show that the base case can be demonstrated to meet ALARP.

In a review of the practices in the Oil and Gas sector, a DNV Technica (1999) report also indicates the use of CBA as the methodology for costing safety measures through a simple yet structured process similar to the UK railway model.

With the comprehensive review of the UK railways duty holder's practices, it is found that there are four main steps established in their guidelines and standards. These steps are traditionally used for determination of safety benefits for the implementation of a system on the operational railways. These include:

- Quantification of the safety risk
- Valuation of safety benefit
- Comparison of options and prioritisation of safety programme
- Option selection and integration into overall project costs

The research into these standards and practices also showed that safety benefits are determined through risk reduction measures targeted at:

- Injuries or fatalities to passengers
- Injuries or fatalities to staff
- Material damage and service disruption

The existing practice of option selection and implementation places a Value of Preventing a Fatality (VPF) based on current VPF values. The approach used simply applies a possible multiplier of 3 to the VPF depending on the maximum risk to an individual. The multiplier of 3, depending on the above factor, addresses the aspect of the ALARP principle which requires safety measures to be implemented unless the cost etc. is disproportionately greater than the safety benefit obtained.

Other studies, such as Komljenovic (2008), Liming (2002) and the practices of the mining and nuclear industries also illustrate the broad use of CBA-related methods. These show the use of probabilistic risk assessment to identify high risk items and the application of Net Present Value to support decisions affecting the allocation and management of plant resources. These studies are not optimisation techniques for risk reduction, but are suggested best practices for attaining cost effective risk reduction. The goals of these techniques (i.e. Risk Informed Asset Management or RIAM models) are geared towards general asset management. RIAM is a process by which analysts review historical performance and develop logic models and data analyses to predict critical decision support figures-of-merit (or metrics) for station managers and executives of electric generation and utility companies. RIAM applies probabilistic safety assessment (PSA) techniques and generates predictions probabilistically so that metrics information can be supplied to managers in terms of probability distributions as well as point estimates. This enables the managers to apply the concept of “confidence levels” in their critical decision-making processes. These metrics include, but are not limited to, the following:

- Profitability
- Projected revenue
- Projected costs
- Asset value
- Safety (catastrophic facility damage frequency and consequences, etc.)

- Power production availability (capacity factor, etc.)
- Efficiency (heat rate), and others

4.2 CBA and Risk Reduction

Applications of CBA in decision making include the use of CBA in Weale (2009) for exploring the effect of cataract operations on eyesight; for public project appraisals Brzozowska (2007); and proposals for transport Elhorst & Oosterhaven (2008). There are even plans for applying CBA to Submarine Decision Support Systems (Bhattacharjee, 2007). Admittedly, CBA has wide and various uses as discussed in Hammond (1966).

This section is not a critique of CBA in all of its applications but makes particular reference to its use in optimising risk reduction with particular emphasis on major engineering projects (in this case risk reduction on the railways). In keeping with the overall objective of this chapter, this section demonstrates in more detail the limitations of CBA in the railway application. The current practice of CBA for safety decision-making is shown to be incapable of dealing with the added complexities of ALARP and financial constraints. It proposes that a comprehensive and systematic function in place of the existing approaches is required to determine efficient risk reduction within budget constraints and in line with regulatory requirements.

Numerous texts and articles have consistently provided topical discussions on the limitations and advantages of applying CBA as we know it today. From a public, government or regulatory standpoint, this is a technique applied to determine the collective alteration from the implementation of a public policy or project with the aim of increasing the quality of public policy decisions using a monetary metric. In CBA measurements, individual welfare is assumed to depend on the satisfaction of individual preferences and social welfare change is measured by observing how much individuals are willing to pay to implement the policy or project. The Willingness to Pay (WTP) approach is used to help inform decisions to go' or 'not go' ahead with a particular policy. The WTP currently applied to market and non-market 'public goods' such as safety risk reduction in critical industries has proved to be a challenge. Cost Effectiveness analysis (CEA) is a subset of the CBA whereby the objective effort of a given policy (e.g. reduction of risk of fatalities on the railways) is directed towards obtaining the lowest cost of reaching the policy goal considering the benefits from other feasible alternatives to a baseline policy.

Most criticism of CBA and associated techniques for achieving cost-effectiveness has centred on CBA's preference-based approach and the view of CBA proponents and analysts alike that system efficacy (mutual risk reduction benefit as a result of the introduction and implementation of a policy or system) can simply be expressed as a comparison of the benefit of the risk reduction in monetary measure and

the cost of the risk reduction measure as is currently practised. Objections have mostly been philosophical, claiming that CBA in engineering applications does not incorporate all factors that influence judgements on the right choice of system. In the past decade, there has been some dynamic movement in the area of research to develop a methodology that addresses the mathematical or scientific concerns that engineering applications of CBA pose when determining a precise economic value. In the wake of the recent economic downturn, the cost of risk reduction measures for recent major investments in infrastructure is more pronounced. It is now common and a key requirement that a decision-maker provide solid reasons for any alteration in a public policy or project.

In estimating the value (benefit/cost) of implementing a system that meet the above requirements, the use of measures based on economic theories (which were initially developed to tackle strictly financial and economic operations) is highly questionable. The flaws resulting from applying these theories to safety critical industries may be disastrous. Other concerns include the use of inappropriate and inconsistent baseline assumptions; application to a wide range of alternatives using simple benefit-cost ratios in place of scientific measurement, discounting measures used in accounting for future benefits and costs, and the monetisation of unquantifiable benefit factors. In exploring the basics of CBA in mainstream publications by Jones Lee (1989), Campbell & Brown (2003), Dasgputa & Pearce (1972), Boardman et al. (2001), Adler and Posner (2000), Schmid (1989), Mishan & Quah (2007), Layard & Glaister (1994), Brent (2006), Dreze & Stern (1987), it is easy to extract that fundamentals of CBA are entrenched in economics and most such theories assume that the satisfaction of individual preferences gives rise to individual well-being.

If the economic theories underlying most of the outstanding work on economic analysis were to be applied to engineering without the application of adequate comprehensive integration of engineering properties, the models will be inaccurate and impracticable. Li et al. (2009) proposed models where expected utility is used as an alternative to CBA in this field. This introduces the risk of equating the introduction of systems (where exposure to risk is not a private matter but a public concern, such as buying cheaper cigarettes).

The concept of utility in most cases when applied to major investment projects in engineering, medical and other safety critical industries has been formed without the concept of ‘value judgement with precise measurements’ – that is, a statement clearly implying that a system X is either good or bad. The numerous ethical criticisms of CBA, ranging from public policies to occupational health and safety issues rage on. Kelman (1981) discusses at length the ethical issues surrounding the use of CBA, specifically on environmental, safety, and health regulation.

The HM Treasury Quantitative Assessment User Guide demands that a full analysis accounts for the impact of uncertainty which leads to Optimism Bias (HM Treasury, 2003). This is defined in the HM Treasury (2003, p.29) as 'a demonstrated systematic tendency for project appraisers to be overly optimistic', which results in an underestimation of scheme costs. Many project parameters are affected by optimism. This is also illustrated in current risk assessment practice (see Chapter 3) where it is established that expert judgements tend to be optimistic. For example, expert analysts tend to overstate benefits and underestimate the timing and level of both capital and operating costs. As expert analysts are uncertain about the future, they naturally tend to ignore new objectives, requirements and risks. However, experience suggests that new objectives, requirements and risks do typically emerge during the course of a project and therefore this tendency should be expected and planned for. The HM Treasury (2003) requires expert analysts to make explicit adjustments for this bias. Conversely, certainty tends to increase progressively from the tender submission to the construction stages of a project. As a result, Optimism Bias is greater earlier in a project's development.

The Department for Transport's Transport Analysis Guidance defines risk as 'the identifiable future situations that could cause overspend or underspend to occur' (Dft, 2013). Risks that could cause underspend are sometimes referred to as opportunities whilst risks that could lead to overspend are sometimes referred to as 'threats'.

A philosophical problem of rationality arises when attempting to establish the 'probability' of an event using expert engineering judgement. Just as we need some level of rationality for willingness to pay under uncertainty as well as certainty, we need rationality hypotheses about probability judgements. These are usually achieved by the theory of subjective probabilities and applications of Bayes' Theorem. The question often asked is – what if the decision makers on railway safety issues do not make their probability judgement in this manner?

4.3 Review of existing strategies for Rational and Optimal Budget allocation to achieve Maximum Risk Reduction

The problem of optimising risk reduction within a fixed budget and regulatory framework is not the classical economic problem of risk under uncertainty. Thus they cannot be solved by the economic theories that are rife and predominant in the financial world and gradually creeping into the safety critical industries.

In an attempt to address uncertainties related to the application of CBA, Li et al. (2009) apply the expected utility theory. This is an alternative approach to optimising risk reduction and a solution to the problem of regulatory decision-making.

4.3.1 Expected Utility – Limitations in use for railway risk reduction applications

It is quite widely accepted in decision analysis that the normative model for expected utility is the theory proposed by von Neumann and Morgenstern. This view is clearly supported in works by Hammond (1988), Harsanyi (1955), Kahneman & Tversky (1979), Eeckout (1996), Broome (1991), de Finetti (1937). Despite being the paradigm for individual choice under objective and subjective uncertainty, experiments by psychologists and economists have discovered several systematic discrepancies leading to the development of alternative models of preferences over uncertain prospects. Notable critical work can be seen in Schmeidler (1989), Allais (1953), Ellsberg (1961), Loomes and Sugden (1982).

Several criticisms, notably Camerer and Kunreuther (1989) criticise the use of expected utility theory for describing the valuation of uncertain outcomes. They also reject the method of comparing distributions of net benefits in which each potential state of the world initiates a particular net benefit and the utility of these net benefits is weighted by their likelihood of occurrence and summed. Their argument is based on the following:

- Individuals tend to systematically underestimate low probability, and high consequence events;
- Individuals' valuation of risk is influenced by their frames of reference and heuristics;

  Perceptions of risky outcomes as well as expected utility are based on the individual's past.

Todinov (2010) demonstrates that the risk of a net loss from risky prospects depends strongly on the number of risk-reward bets in the risky prospect. He demonstrated that two risky prospect with the same expected profit can be associated with very different levels of risk due to the number of risk-reward bets in them. Todinov also demonstrated that the risk associated with a risky prospect can be reduced significantly by splitting it into a number of risk-reward bets, each characterised by the same probability of success but by a proportionally smaller benefit and cost. This study shows that even with a full knowledge related to the likelihood of an event and its consequences, and without the existence of subjective bias when making a decision, the maximum expected utility principle proposed for optimising risk reduction in Li J et al. (2009) is fundamentally flawed. This results in the acceptance of significant risks, associated with grave losses in the case of a small number of risk-reward bets in a risky prospect.

The statistical **law of large numbers** supports this argument. If we consider a number of independent but broadly similar risk-reward bets. In some cases, the net benefit may fall short of its expected value, in other cases; the net benefit may exceed expected value. A large number of risk-reward bets will tend to balance out loss and gains resulting in net gain not far from the expected value. For small number of risk-reward bets, this is not guaranteed and large deviations are to be expected.

Dasgputa & Pearce (1972) used examples involving expected utility, variance and law of large numbers to express a similar view. Let us consider μ_i as the utility of a possible outcome and ρ its probability of occurrence if a particular decision is taken. The first moment of probability of the decision, which is a measure of central tendency called the arithmetic mean or expected value can be expressed as

$$\sum \rho_i \mu_i = \mu \qquad (4.1)$$

The second moment of probability, the variance, can be expressed as $\sum \rho_i (\mu_i - \mu)^2$. The y^{th} moment is then defined as:

$$\sum \rho_i (\mu_i - \mu)^\gamma \qquad (4.2)$$

For most practical applications, we can effectively use the first two moments for comparisons as practised in expected utility theory and some CBA applications.

One of Marschak's axioms on expected utility also implies that there must be at least four similar prospects to prove the Expected Utility Theorem (Marschak, 1950). Dasgputa & Pearce (1972) cite other notable expected utility critiques and conclude that in practice, economists generally confine their attention to more routine situations. This means that the utility function is bounded. The assumption of bounded utility automatically excludes choice among alternatives involving consequences significantly worse or better than others.

On the upside, there has been extensive work done discussing and attempting to address biases in subjective measurements of risk in economics and engineering. These include work presented in Jones-Lee (1976), Trevor et al. (1998), Beattie et al. (1998), Olivier et al. (2004), RSSB (2006), Lind et al. (1997), Arkes (1991), Fischhoff (1982). These may apply to the derivation of quantities from hazard management to quantified risk assessments and policy or risk regulations.

Economics theory on the expected utility has evolved significantly since proposed by von Neuman & Morgenstein (1947). Notable economists who have made attempts at improving the Expected Utility Theory include Markowitz (1952), Tversky and Kahneman (1992). Markowitz proposed a new model of utility. Markowitz's model, unlike in standard expected utility theory assumes that the decision maker was initially risk-loving then risk-averse over gains whilst initially risk-averse then risk-seeking over losses. Though perhaps not widely appreciated, the decision maker was also assumed to be loss averse. Markowitz model explains a variety of experimental evidence not consistent with the expected utility theory. Cumulative Prospect Theory of Kahneman and Tversky (1979) is considered to be the major alternative to expected utility theory having superseded Markowitz's model.

4.3.2 Cost Benefit Analysis – Limitations

CBA in its pure form requires that all impacts relevant to efficiency be quantified and made commensurate through monetisation to make use of the Pareto principle through the calculation of benefits. This makes CBA difficult as limitations in theory; data or analytical resources may make it impossible to measure and value the impacts of the introduction of a system. Empirical measures can have varying degrees of accuracy and the decision to quantify and with what degree of effort, should reflect the value of the increased precision that can be obtained and the costs of obtaining it. CEA , used when all the impacts cannot be monetised in a CBA, is an alternative, abridged version, that lacks the science to provide a decision-making framework for selecting efficient risk reduction measures. In the case of distributionally-weighted CBA used for achieving maximisation of net benefits, the analyst's major problem is obtaining an appropriate and acceptable set of weights.

The accuracy of a CBA depends for the most part on the stage of the project on which it is undertaken (Todinov, 2001). Errors in CBA decline as the analysis is undertaken during the latter stages of a project. A CBA conducted at the concept stage is subject to numerous compounded errors. These may arise for many reasons most commonly, where managers systematically overestimate benefits and underestimate costs, which are termed strategic bias. However, logically and in practice, most CBA occur at the initiation or concept stage. This exposes the project or undertaking to some significant losses, considering the inadequacies already outlined in this chapter. Weli and Todinov (2013b) also provide some exhaustive information on the impact of incorrect application of techniques at these initial stages. Boardman et al. (2006) highlight four fundamental CBA flaws including:

- Omission errors;
- Forecasting errors arising from inherent difficulties and due to factors such as predicting technological change, cognitive bias, changing project specifications and for strategic reasons;
- Valuation errors as a result of inaccurate estimates of the value of criteria such as time, lives saved and valuation errors from unanticipated relative price changes etc.;
- Measurement errors with a tendency to assume that once an impact has occurred, all uncertainty associated with the impact is removed. The extent of problems resulting from measurement errors largely depends on the equipment or technology used and on the robustness of the statistical or econometric methods.

Boardman et al. (2006) acknowledge that these problems have received little specific attention within CBA. This is likely due to the difficulty of addressing stringent data requirements and the need for strong underlying assumptions placed on statistical methods used for handling the errors.

Other well reported problems in the use of CBA are highlighted in Maciariello (1975). In particular, this study discussed the problem of interpersonal utility comparisons, underlining the difficulty in measuring utility and the incorrect approximations when using benefits to quantify utility. The change in monetary benefits as a proxy for a change in utility results in substantial inaccuracies with the application of CBA. This problem was illustrated using the Kaldor-Hicks criterion, which runs into utility comparison problems. These analyses showed how CBA may move us away from, rather than towards an optimum value. Maciariello further concludes that the requirements of pure economic theory are simply too demanding for most practical benefit-cost studies and that compromises are required at virtually every step of a typical study. In a rather distinctive way, Kelman (1981) further provides an ethical critique of CBA including its misuse in areas of environmental, safety and health regulations.

4.3.3 Cost Benefit Analysis – railway risk reduction application constraints

By introducing the economic cost-benefit analysis method, railway decision-makers and safety analysts consider the accident costs and risk reduction using 'Do-something' and 'Do-nothing' scenarios. This methodology in practice does not require prioritisation and in some business cases it adopts the prevention-first method, i.e. only considers measures for reducing the likelihood of failure with the consequences in such an event treated as an after-thought. The economic cost-benefit approach uses a simple ratio to review potential risk reduction measures and selection is made on the basis of comparisons between the net costs of the risk reduction measure and the benefits. If the net benefits outweigh the costs, the introduction of the risk reduction measure is beneficial to the railways and passengers. The risk reduction measures are subsequently ranked according to the estimated cost-benefit ratio.

Figure 15 shows the steps for deriving the benefit and cost ratio. The events and contributors to the railway major accidents are extracted from existing safety analysis such as quantified risk assessments, hazard and operability studies or workshops. In some cases existing accident data is filtered and those relevant to the specific application are identified and used.

The distribution of contributions to the overall accident is potentially a challenge as this may not be adequately captured in fault trees or in data provided for risk reduction analysis. This analysis however assumes that the set of risk contributors used provides a sufficient representation of the accident as the information is extracted from different studies with corresponding data.

The costs of implementation are provided from economic safety studies undertaken for a recent project on the line section under study. The data covers signalling, communications, trains and other systems. The cost data is a combination of acquisition, installation and implementation and where available, the

maintenance of the safety system under consideration. To ensure economic calculations for removed risk are based on the same premise as the estimated costs, the risk reduction as a measure of likelihood and consequence (cost) is provided in monetary terms. The VPF value of £1.7 million (i.e. for 2012 values) and fatality rates for the different accidents are employed for estimating the cost of accidents. The removed risk is then the benefit of implementing the measure and provided as the difference between the cost of accident and cost of risk reduction.

Applying risk reduction measures to different accident contributors will have different effect on the accident risk reduction. A good example is the application of 'Overlap Extensions'. These can be used to effectively reduce the contributions to Collisions between Trains such as SPADs, compromised overlaps, poor wheel-rail friction/interface, failure of emergency braking, wrong direction movements, speeding (signal) overruns, etc. However, the overlap extension will also have variations in the magnitude of risk reduction provided to the different contributors to collision between trains, and is, therefore, potentially only cost effective in some scenarios, not all.

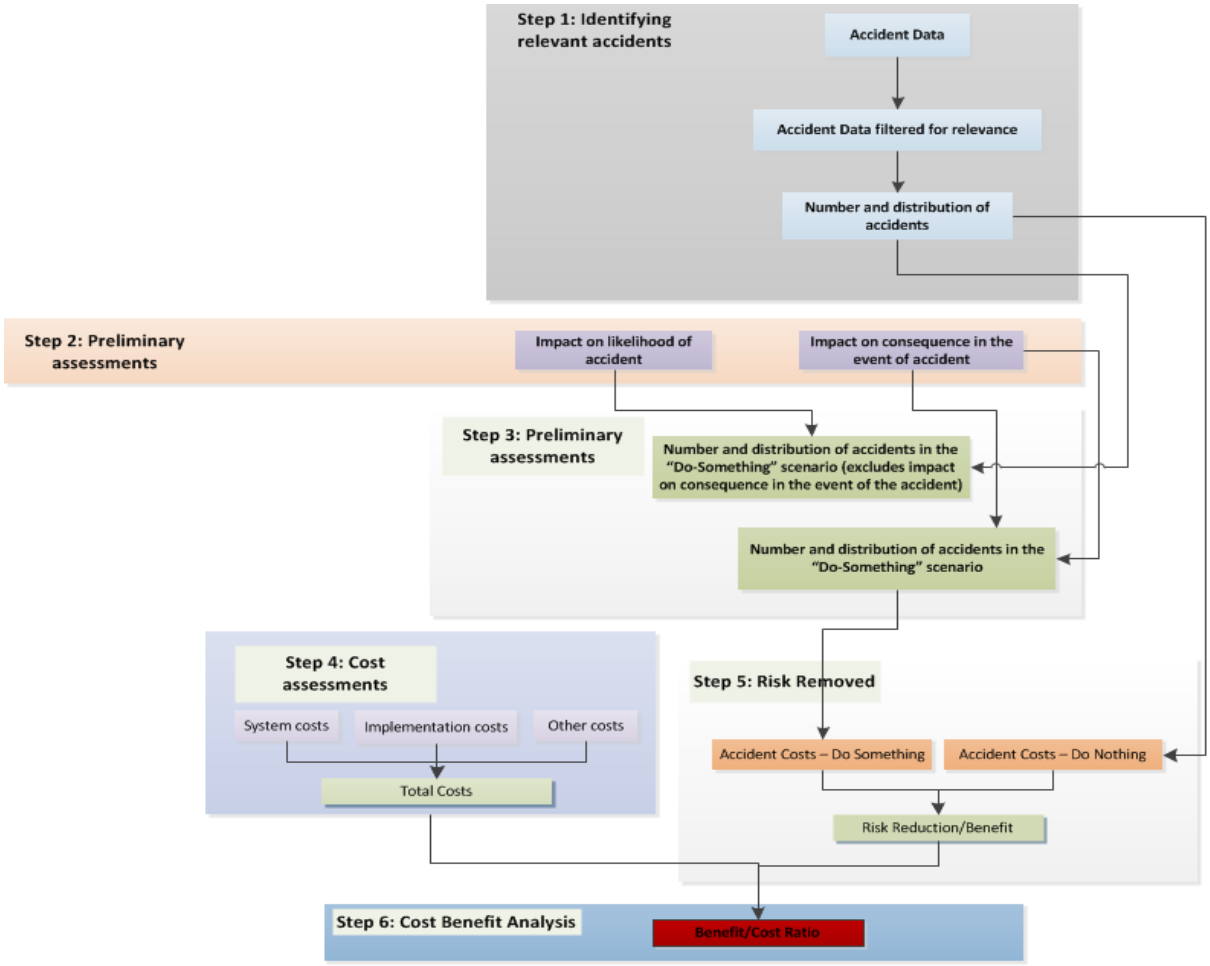


Figure 15: Cost Benefit Analysis – selection of systems for risk reduction

The flaws with this approach are significant and could lead to significant inaccuracies in the results. Currently, it fails to consider all risk reducing measures as integrated measures to achieve effective risk reduction. The obvious practical flaw with the application of this method is that the preventive measures only target the minimisation of the likelihood of risk actualisation. Considering the inevitable uncertainties in accident or reliability data and the level of engineering expert judgement needed in these evaluations, the resulting decisions will often be incorrect and potentially catastrophic. Any confidence in the effectiveness of the risk reduction measures selected as a result of this approach is also dampened by the heavy reliance on quantified estimates associated with large uncertainty. The uncertainty varies and increases with the extensive use of the estimates. For quantification to accurately play a major part in any risk evaluation, a study that provides a degree of confidence must be derived from extensive and trustworthy accident data collected over a period of time, within a similar environment. This suggests a reactive approach to accident risk reduction and raises the question of how railway modifications with associated interfaces (new and existing systems) will be captured. This adds to an erosion of confidence in data collection, recording and usage.

For a practical illustration, let us consider a set of risk reduction options addressing one of the most common and most researched incidents: signals passed at danger (SPAD) or signal overruns, potentially leading to a collision.

1. Automatic Train Operation – Train control and protection systems (by removing requirement for signals and driver related failures)
2. Overlap extension
3. SPAD incident response plan/system – operating procedures and availability of first aid
4. Signalling modifications to align with sighting constraints
5. Speed restrictions
6. Driver and line controller training
7. Adhesion/wheel slide protection systems
8. Trip-cock positions re-examined and potentially relocated
9. Introduction of efficient speed control systems
10. Introduction of more reliable brake control systems
11. In-cab design – improvements to train cab ergonomics
12. Train Protection and Warning System (TPWS)
13. Modifications to testing and maintenance regime – extend operational testing for existing infrastructure
14. Emergency timetable for addressing severe disruption following an incident

The options presented have varying risk reduction benefits at different costs. Some are preventive risk reduction measures. The primary task of these measures is to reduce the likelihood of SPADs contributing to the risk of collisions. The current practice of risk reduction raises many questions which are not limited to the list below:

- Considering a fixed and in some cases, diminishing budget, what assurance can be obtained from a decision based on risk reduction if the preventive measures alone are considered?
- What level of confidence can we achieve with the use of any of these considering that the existing methodology is heavily based on quantitative targets with an increasing degree of uncertainty as reliability, accident and statistical data are employed to demonstrate tolerability and ALARP?
- If effectiveness is only considered on prevention-first methods with minimal consideration of protective measures, what level of uncertainty in the initial analysis is representative of consequence/cost for considering protection measures, i.e. what level of prevention can we ideally look to achieve (or is permitted) prior to the use of protection measures?
- If a measure regarded as preventive is selected, what criteria support the selection? Is it enough to use the cost vs. risk reduction benefit to make the decision on which risk reduction measure to select?
- The first and most pressing question is – on what grounds have we classified these as preventive or protective?

As shown in previous discussions in this chapter, the norm is to extract data from historical data of similar systems, standards and operational environment. However, for many events, appropriate historical data is unlikely to be available. Without sufficient and thorough assessment of the application, the use of tools in options selection that relies heavily on historical data could potentially derail a decision-maker and lead to catastrophic consequences. The detrimental effect of such cases is addressed in Weli and Todinov (2013a). The paper presents a real-life scenario which has been an issue in all UK applications of the axle counter product for over 10 years. The introduction of axle counters to achieve position detection for trains as a replacement for 'track circuits' is an illustration of the catastrophic effect of a cost–benefit approach reliant on historical data. Train position detection is a primary requirement for a safe operation of the railways. Due to lack of historical data regarding the frequency of failure of the axle counters, the accident history of the track circuit was used in the cost–benefit analysis. This revealed a net benefit of £500 per unit from this use. However, the historical data related to track circuits failed to reveal the

following dangerous failure scenarios: (i) broken rails could easily be detected by the track circuit device but not by the axle counters; and (ii) rail grinding wagons frequently brake axle counter heads, which makes them unsuitable for operation. The problems arise from an inability to detect broken tracks and, in addition, the axle counter heads have to be re-calibrated and re-installed after grinding operations. The result is increased risk levels for passengers, delays and other severe operational challenges.

4.4 Existing Railway Safety Budget allocation Strategy

A major and on-going criticism of existing safety decision-making by analysts, regulatory bodies and organisations, is the conventional estimation of multiple-goal activities by single, technically convenient measures. The challenge in safety budget allocation is a multi-objective problem (similarly encountered in daily industry investment and other critical decision making activities). It potentially involves an array of conflicting objectives such as cost, time, regulatory policies, profitability and interface risks, short-term, intermediate and long-term consequences. This supports the case that only a systematic and comprehensive approach can deliver the required maximum risk reduction.

Most railway safety decision-making company guidelines in this specific area apply the prevention-first principle. This ensures that by eliminating the likelihood of risk materialisation, the risk of the accident can be significantly reduced. This prioritisation of preventive risk reduction measures, as rudimentary as it seems, is provided in the HSE document R2P2 (HSE, 2001c) and widely used in current practice. It is unsuitable for safety-critical industries such as railways as it is used to determine the vital factors that influence the risk reduction, without complete consideration of other potentially effective risk reduction measures. For example, protection measures are only considered if the preventive measures do not reduce the risk to a tolerable level in line with ALARP principles. The selected risk reduction measures are then taken forward for cost considerations i.e., the risk reduction measures with greater impact on preventing the accident are then assessed based on their cost and magnitude of risk reduction. The risk of neglecting some essential properties of other measures is significant. If we are provided with two preventive risk reduction measures at a cost of £4 million with combined risk reduction of £1 million, six protection measures at a cost of £1 million, and associated risk reduction of £4 million, the prevention-first principle could theoretically be blindly applied. Failure to consider risk protection measures is a vital weakness which increases the overall risk in cases where the potential hazards cannot be properly evaluated (unknown unknowns) and the only mitigating barrier against accidents caused by them is the risk protection option.

4.4.1 The business case for risk reduction

Business cases for safety projects require that both the willingness to pay and the cost of alternative measure(s) are considered. Cost Benefit Analysis is used extensively on the railways for providing a

business case enabling authorising bodies within the industry to make informed decisions on whether to approve proposals for change. Business case appraisals are often part of operating most successful businesses worldwide, not least the UK railway industry with its enormous size and importance.

A standard requirement from railway operators is that any case put forward must be argued on its merits and on the features of the options to be evaluated. All cases are required in quantified formats although the methods of quantification may be different for each case. In reducing the occurrence of incidents which could lead to loss of life or injury, CBA is used as part of the risk assessment process, which may lead to major operational changes (see Figure 16). The cost of an accident or incident in this case is expressed in financial terms, facilitating comparisons between safety benefits with expenditure and arriving at an estimate of whether or not the latter is worthwhile. HSE (1974) stipulates that the cost of reducing hazards must be increased to the point where the residual risk is ALARP.

As surmised in one of the UK railway operator business development manuals, CBA related to safety risk is presented using this simple statement:

> "*If the probable frequency (expressed in number per annum) of an event occurring and the probable outcome (expressed financially) if the event occurred are known, then the product of these two numbers is the probable cost per annum of the risk. If as a result of the expenditure, the magnitude of either or both of these two quantities is reduced, then the reduction in annual costs can be determined. The cost determined can then be compared against the cost of eliminating the hazard and the overall system operational effect.*"

HM Treasury (2003) also known as the Green Book is designed to promote efficient policy development and resource allocation across government and government agencies. The Green Book supports effective resource allocation by ensuring that decision-making on policies, programmes or projects are improved through alignment with government priorities and public expectations – usually a difficult balance to achieve. As provided in the Green Book, this is achieved through:

- Identifying other possible approaches which may achieve similar results;
- Wherever feasible, attributing monetary values to all impacts of any proposed policy, project or programme;
- Performing an assessment of the costs and benefits for relevant options

HSE (2001c), RSSB (2007b) and railway industry standards in their guidelines for risk management and cost valuations of risk, propose basic steps to adequately reduce risks on projects. The UK railways apply six basic steps for achieving optimal risk reduction, which informs decisions for option selection and are summarised below as:

- Understand Project Purpose and Aims
- Hazard Identification
- Risk Quantification (likelihood and consequence)
- Risk Evaluation (in terms of ALARP or risk ranking)
- Identify Risk Mitigation Options (and costs and residual risks)
- Determine optimal Option (by cost benefit analysis)

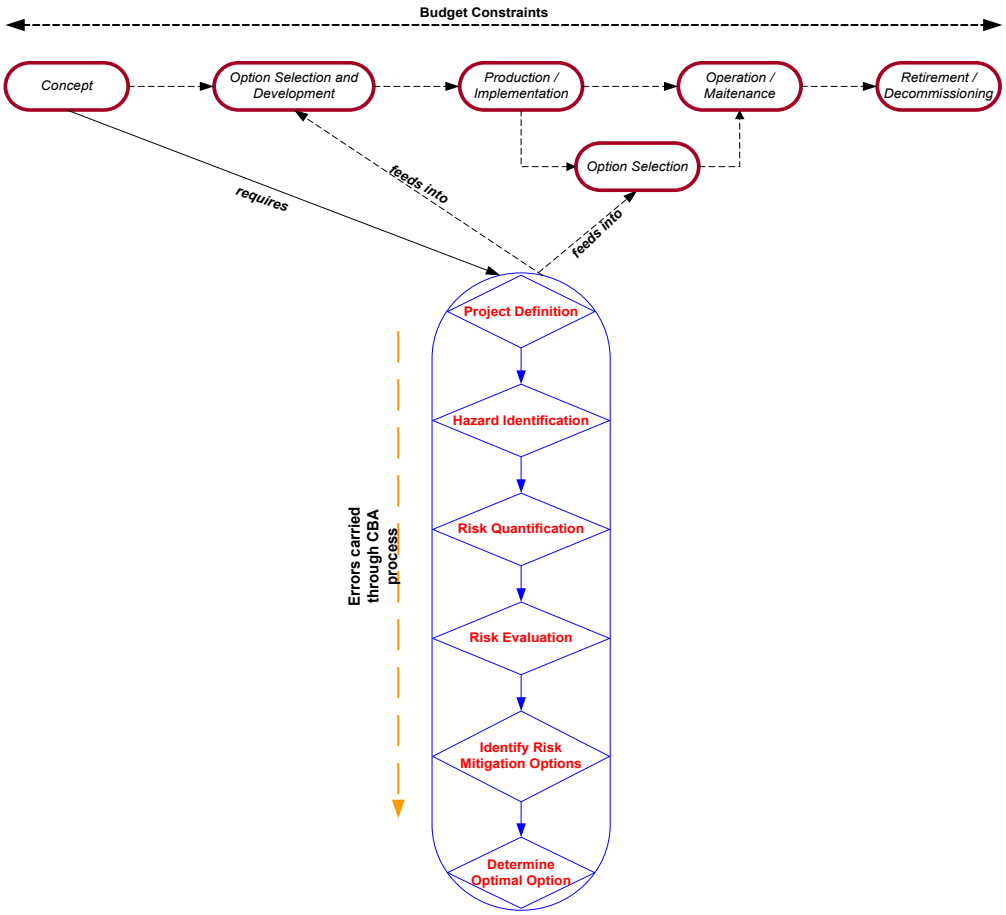


Figure 16: Engineering Lifecycle and CBA application

The approach to risk mitigation depends on the steps taken prior to option selection through the engineering lifecycle as shown in Figure 16. Options for risk mitigation should be considered together with their benefit (in terms of risk reduction and the resulting residual risk) and the cost, time and implementation effort.

From a number of possible options (which will include a 'Do Nothing' option) optimum risk mitigation (or combination of risk reduction measures) is chosen for implementation. Furthermore, synergies between risk reduction measures should be taken into account. In some cases, one option can reduce various risks.

The residual (i.e. remaining) risk and the cost of the risk reduction measure is also taken into consideration. Risk reduction is normally considered to fall into the following categories:

- Avoid (i.e. do something else)
- Transfer (e.g. insure, sub-contract, transfer to another party in the contract, etc. Note that the duty holder cannot transfer Health and Safety or environmental risks.)
- Retain (hold i.e. do nothing)
- Reduce:
- Reduce the Likelihood of occurrence (e.g. use greater Factor of Safety)
- Reduce the Impact if failure occurs
- Rescue (e.g. emergency planning)

In theory, the evaluation of risk and cost should be more definite and precise as a project progresses. With the current practice for selecting most cost effective measures for risk reduction, the question remains – is the CBA methodology currently practised adequately optimising risk reduction considering the lapses and flaws inherent in the information used for CBA? Is the CBA methodology currently in practice appropriately optimising options identified?

The limitations of the current budget allocation technique and practices have been demonstrated in this chapter to be a challenge with the widely adopted CBA. Brent (2006) presents different methods of measurement of tangibles and intangibles during a CBA study: the travel cost method and the revealed preference approach using random utility theory. Brent also surveys the contentious realm of valuing human life by the traditional methods, which are variants of the human capital approach. However, Mishan (1976) maintains that neither of the traditional methods corresponds with the individualistic value judgement behind CBA. The valuation of human life using cost-benefit issues is prominent in health regulations, safety regulations, welfare policy, disease inoculation, research and development into many kinds of new products, and in many other areas of government policy that affect decisions about who lives and who dies. CBA usually treats the value of life by measuring the value of risks of death. Economists can examine how much an individual will pay to lower the risk of dying in a car accident or a flight. Several critics have questioned the suitability of using these procedures. These critics question whether we do in fact have good measures of the value of risk reduction. Data are usually taken from market demands for safety equipment (such as helmets) or salary for especially risky jobs. Neither of these can provide an accurate assessment of risk reduction.

The cost-benefit method that suggests using either willingness to pay or willingness to be paid criteria is shown in a typical example of health economics where a mountaineer is lost and resources are being

devoted to rescue. How far should society go in saving a set of known victims and in a case where the victim knowingly took the risk? If an individual or group of individuals suffers from a potentially fatal disease, how much resources should be devoted to trying to find a cure? Star (1969) observes that people accept 1,000 times more risk when they choose the activity; hence pay more than when it occurs as a result of others' actions. The emphasis on the value of risk reduction by the economist using CBA presents a fundamental difficulty for cost benefit methods. Typical risk reduction options involve cases where we know that an identifiable individual will die unless specific action is taken to prevent this outcome. The inability of CBA to handle cases of certain death raises questions about potential death as well, that is, about valuing risk reduction. Economic methods for valuing human life therefore represent a value judgment on the part of the economist, rather than a fully objective application of the cost-benefit method.

Several authors, researchers and organisations have undertaken studies on the business case and allocation of budgets in different fields and cite CBA, as it is widely used in all areas of business. These include Blackorby & Donaldson (1990), Dreze & Stern (1987), Robin (1974), Adler & Posner (2000) and Jones-Lee (1976). In the selection and allocation of budgets for risk reduction, any *additional* safety measures on a project are considered by comparing:

- The cost of implementing the measure.
- The benefit of the measure, in terms of the risk-factored cost of the accidents it would avert.

Recently, attempts have been made to make the comparison in terms of risks to life, but these are not yet generally accepted. The determination of the total annual cost of risk reduction measures employed usually includes:

- Costs of capital investment (e.g. purchase and installation of new safety hardware) written-off over an assumed working lifetime at an appropriate discount
- Operating expenditure (e.g. on annual safety training, extra staff, maintenance etc.).
- Lost profits (before tax) if the measure involves withdrawing from an activity altogether.
- Extra operating costs from safer working practices are not normally included, as they are assumed to be balanced by cost savings from the generally more efficient operation.

The cost of accidents averted by the risk reducing measures includes:

- The value of life of people killed;
- The cost of hospital treatment, lost production and human costs to people injured.
- The cost of damage to property;

- The business interruption costs, mainly lost production, but also including the damage to company reputation resulting from a major accident. These may be large and particularly difficult to estimate.

Some approaches to CBA incorporate such factors for gross disproportion in the valuation of risk. Others use a baseline valuation and separate gross disproportion factors.

4.5 Evaluation of the Existing Railway Safety Budget allocation Strategy

At the request of the ORR, the Health and Safety Laboratory researched the development of an asset management model for UK railway safety allowing the UK to allocate spending on rail safety to maximum economic effect. This resulted in the report by the Health and Safety Laboratory (HSL, 2005) proposing an asset management model focussed on the UK railways. The report proposes an outline for a robust model to support safety budget allocation and suggests eight key steps:

- ***Safety Policy*** – The establishment of high-level safety targets for the UK rail industry, which will necessarily require top management commitment.
- ***Identification and prioritisation*** – The use of Quantified Risk Assessment to identify assets critical to achieving the high level safety targets
- ***Setting Performance Objectives*** – Deducing the performance required of an asset in order to meet the high-level safety targets.
- ***Maintenance Tasks and Procurement*** – At this stage, the different approaches to maintenance and procurement i.e. life-cycle assessment is considered.
- ***Immediate Review*** - This step allows a high level ALARP assessment to be made, with policy (and perhaps legal) implications for HMRI
- ***Audit*** – This gives confidence that the model has been implemented consistently and correctly across the rail system.
- ***Implementation***
- ***Periodic Review*** – This is particularly relevant to this study as it underlines the required task of reviewing existing systems / processes when there are major changes to the railway e.g. the introduction of new regulations, drastic changes in budget or priority, new infrastructure.

Despite the benefits outlined in the report, the model is similar in theory and practice to the Health and Safety Executive publication 'Successful Health and Safety Management' based on the plan-do-check management model (HSE, 1997). This also represents the principle of continual improvement as denoted in the British Standard for quality assurance systems, a standard format for existing Safety Cases in accordance with Railway (Safety Case) 2000 Regulations (ORR, 2013) and general safety cases used in the high-risk engineering industry. However, the model and report fail to make good on claims of proposing an optimal approach to managing assets with great potential for saving resources or deploying them effectively.

The report lacks the depth required to claim that the proposed framework is a 'grand unifying theory' for optimising spending on the railways as railway safety is not comprehensively addressed. The report however sheds some light at a peripheral level on the connection between policy and regulatory changes to railway safety business decisions which requires further study to highlight the need for aligning safety investments to safety targets and subsequently to government or industry regulations. In spite of the report's high level approach to asset management regarding safety, it does note that an understanding of key features affecting safety performance (i.e. the need for lower level activities such as asset registers, QRA, accurate costing and procurement to support maintenance and downtime) is required to optimise safety costs. This, as noted rather than emphasised in the report, is the essential bottom-up approach to safety budgeting to ensure a truly 'unifying' framework for safety budgeting.

4.6 Decisions to support maximum risk reduction and budget allocation

In Chapters 3 and 4, this thesis extensively highlighted the key areas that distort risk management on the railways. These are currently the practices, processes and tools that misrepresent railway risks and risk reduction. This necessitates a fundamental change to risk management in order to effectively support the railway operational safety case.

The main challenge is the development of a framework that gives the decision maker confidence that the effective risk reduction measures are considered – including the correct application of risk reduction measures at a reasonable cost. When embarking on this study, some careful thought was given to the typical questions that inundate a decision-maker in this area. The questions are comprehensive, however not exhaustive, and in no particular order. These are presented as an overview of some of the fundamental challenges to applying risk reduction measures which have not been addressed in current practice:

1. Is there a clear understanding of what preventive and protective risk reduction measures apply, and in what cases are these measures applied for cost effective risk reduction?

2. What risk reduction measures do we invest in and how is this achieved for particular railway accidents or accident scenarios?
3. Assuming we have identified and know the risks or contributors to a major accident, is the introduction and implementation of only preventive risk reducing measures sufficient to reduce the risk to ALARP?
4. In cases where the risk cannot be easily quantified, how are risk reduction measures applied?
5. With varying degrees of uncertainty in data and subsequent sensitivity analysis, what methods reduce the underestimation or overestimation of the magnitude of risk reduction and costs associated with selecting the risk-reduction measures?
6. In new railway developments with associated scrutiny on costs, is it worth investing more in measures that prevent the risk or protect against the risks of accidents?
7. What is the most effective way of allocating budgets: how are the preventive and protective risk reduction measures for a particular risk distributed or allocated?
8. How are risk reduction measures which act in parallel to other measures determined, and what is the contribution of these parallel measures to the overall risk reduction objective?
9. In marginal reduction cases, mostly cases encountered on the railways, how are preventive or protective measures appropriately employed?
10. What important cost considerations drive the decisions on preventive or protective measures?

In order to achieve cost effective risk reduction as a minimum, the effort required for supporting the selection and implementation of measures must be directed towards ensuring a structure and clarity to the risk reduction measures. By emphasising a better understanding of the measures based on underlying generic principles, allocating appropriate measures to particular risks or risk scenarios for effective reduction can be achieved. Without this fundamental clarity and systematisation, it is impossible to see how the aspects of successful risk management can be efficiently addressed.

Consequently, Chapters 5 and 6 present the fundamentals that can adequately support any claims to cost effective risk reduction. This comprehensive baseline study offers the required guidance for the essential understanding of risk reduction measures in railway applications. Chapters 5 and 6 establish the basis for an assured selection of maximum risk reduction measures within budget constraints.

Chapter 5 Preventive Principles and Techniques for Reducing the Risk in the Railway Industry

Chapters 5 and 6 present the basics (i.e. fundamentals of risk reduction application) that can support further efforts on cost effective risk reduction and subsequently, their maximisation under budget constraints. Chapter 5 specifically focuses on preventive risk reduction measures. Preventive risk reduction measures are applied to reduce the likelihood of an event/accident. As established in chapters 3 and 4, the selection of measures to provide practical and verifiable cost effective risk reduction based on essential railway risk reduction requirements is necessary to achieve maximum risk reduction.

Using generic risk reduction principles, the measures applied within the railway network are clearly outlined. This provides the decision-maker with the vital understanding for effective application of risk reduction measures in specific applications (reducing the likelihood of an event/accident).

The distinct mapping of railway preventive risk reduction measures to preventive risk reduction principles is a first for the UK railway industry. This chapter goes further to present the generic costs, constraints and considerations associated with implementing separate measures for the major accidents – Platform Train Incidents (PTI), Collision Between Trains (CBT) and Derailments.

5.1 Fundamentals to maximising risk reduction given fixed budget

Currently, no practical and verifiable alternative exists for selecting risk-reduction measures. This study moves on to the systematic and comprehensive approaches that avoid the existing heavy reliance on historical accident or failure data. In order to demonstrate approaches that will support the decision maker in selecting and optimising cost effective risk reduction measures that consider budget constraints, the essential principles adopted in this thesis as fundamental assumptions in cost effective risk reduction are:

1. The selection and effective application of risk reduction measures will depend on a thorough understanding of:
    - The risk reduction measures' strengths and weaknesses
    - The application environment
    - Interaction between the risk reduction measure and the application
2. Some risk reduction measures have both preventive and protective characteristics. The feature that dominates the specific risk reduction objective is the guidance on the effective application of such measures.

3. Risk reduction achieved during the initiation or evaluation stages of a project must be sustained throughout the operational stages. The functional interfaces and dependencies between people, processes and equipment must be well understood and incorporated in the initial evaluations and carried through implementation.

5.2 Preventive Risk Reduction Requirements, Principles and Systems

The basic UK railway safety processes and practices are developed from a combination of regulatory and specific infrastructure owner requirements. These requirements are designed to ensure that the major accident risks or top-level events are prevented by the application of the ALARP principle. The safe operation of a train is a fundamental requirement. This becomes more complex when modifications and new technologies are introduced.

5.2.1 Risk Reduction Requirements

As the recent improvements in railway technology contribute to automation in fixed and moving block systems, the latter being more of the case today, the operational safety philosophy i.e. a checked-redundant, fail-safe principle is built into the design and development of these systems. The overarching requirement of 'safe operation' of trains can be further analysed by re-classifying functions:

- Implementation of effective train separation
- Enforcement of train speed limit and travel direction
- Control of platform and train doors
- Train location through point and route locking

Reducing the major accident risks is achieved by reducing the likelihood of the accidents by:

- Preventing risks such as collision between trains,
- Preventing risks of collision between trains and fixed objects,
- Preventing risks of derailments due to over-speed and
- Prevention of safety risks to staff and passengers.

To further explain and validate these primary functions or relationships, we consider the 2008 accident data for a given railway line presented in Figure 17. The data is based on a 70km railway line with 34 stations, approximately 33 - 35 trains operating daily, 60 – 70km/hour line speed and 54 million journeys per year.

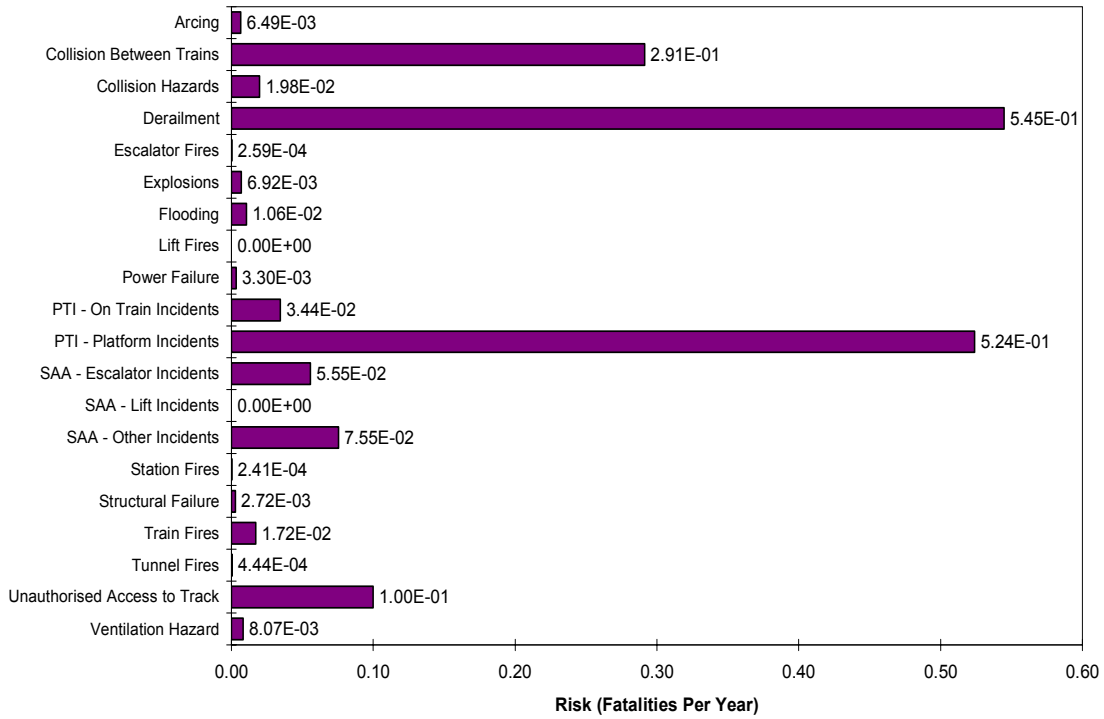


Figure 17: Railway Line Risk Profile (2008)

Figure 17 illustrates that the most significant accident risks – Collision between trains, Derailment and Platform Train Interface (Platform incidents) are the consequences of deviations from the primary functions. This suggests that for effective risk reduction on the line section used for this study, a thorough assessment of the preventive measures that reduce the likelihood of these primary accident risks is required. The assessment will help facilitate further understanding of risk reduction within the application. Subsequently, a robust strategy to support maximum risk reduction within constraints such as budgets is developed.

In the analysis of a system for accident prevention, all elements must be taken into consideration, i.e. software, hardware, human factors, socio-political influences and environmental issues, throughout the life cycle of the system. Information should be reliable and complete. Any effort towards developing a framework for maximum risk reduction must consider systems and human failures in the application of preventive measures. This approach is further supported by considering typical contributory events presented in the Tables 10 to 12:

Table 10: Contributors to the Collision Between Trains

Major Accident	Example Risk Contributors
Collision Between Trains	Brake Trigger System Failure
	Train runs away
	Speed Control After Trip (SCAT) failure
	Signal Wrong Side Failure (WSF). A 'wrong side failure' is a signal failure that leads to an

Major Accident	Example Risk Contributors
	incident/accident.
	Compromised overlap. An overlap is the distance provided for a train to stop short of any obstruction if it fails to stop at the signal
	Poor wheel/rail friction
	Driver or operator error
	Signal Passed at Danger (SPAD)
	Collision subsequent to a collision
	Train radio system/communications failure
	Emergency brake failure
	Track circuit/train position detection failure
	Wrong direction train movement

Table 11: Contributors to the Derailment accident

Major Accident	Example Risk Contributors
Derailment	Defective wheel
	Excessive speed
	Suspension failure
	Emergency exit
	Side swipe
	Poor wheel/rail friction
	Track buckle
	Shoe caught under the conductor rail
	Loss of train detection
	Collision with object – object on track

Table 12: Contributors to Platform Train Incidents (Platform only accidents)

Major Accident	Example Risk Contributors
Platform Train Incidents	Crowded platform – inhibits driver's view
	Curved platform – inhibits driver's view
	Door dampener failure – doors closing with excessive force
	Passenger falls from platform
	Passenger falls between cars
	Falls onto platform from train
	Trespass
	Passenger strikes/falls against train
	Person pushed from platform
	Failure to activate emergency stop buttons or alarms

Additional application definitions of these contributors are presented in discussions on the preventive measures in this chapter, and protective risk reduction measures in Chapter 6. An introduction to fundamental principles, associated processes, systems and applications are presented. Section 5.2.2 introduces generic preventive principles and their connection to the fundamental railway safety requirements.

5.2.2 Preventive Risk Reduction Principles

Figure 18 presents a set of preventive risk reduction principles. Subsequent sections provide detailed examples with additional evidence of application limitations and strengths.

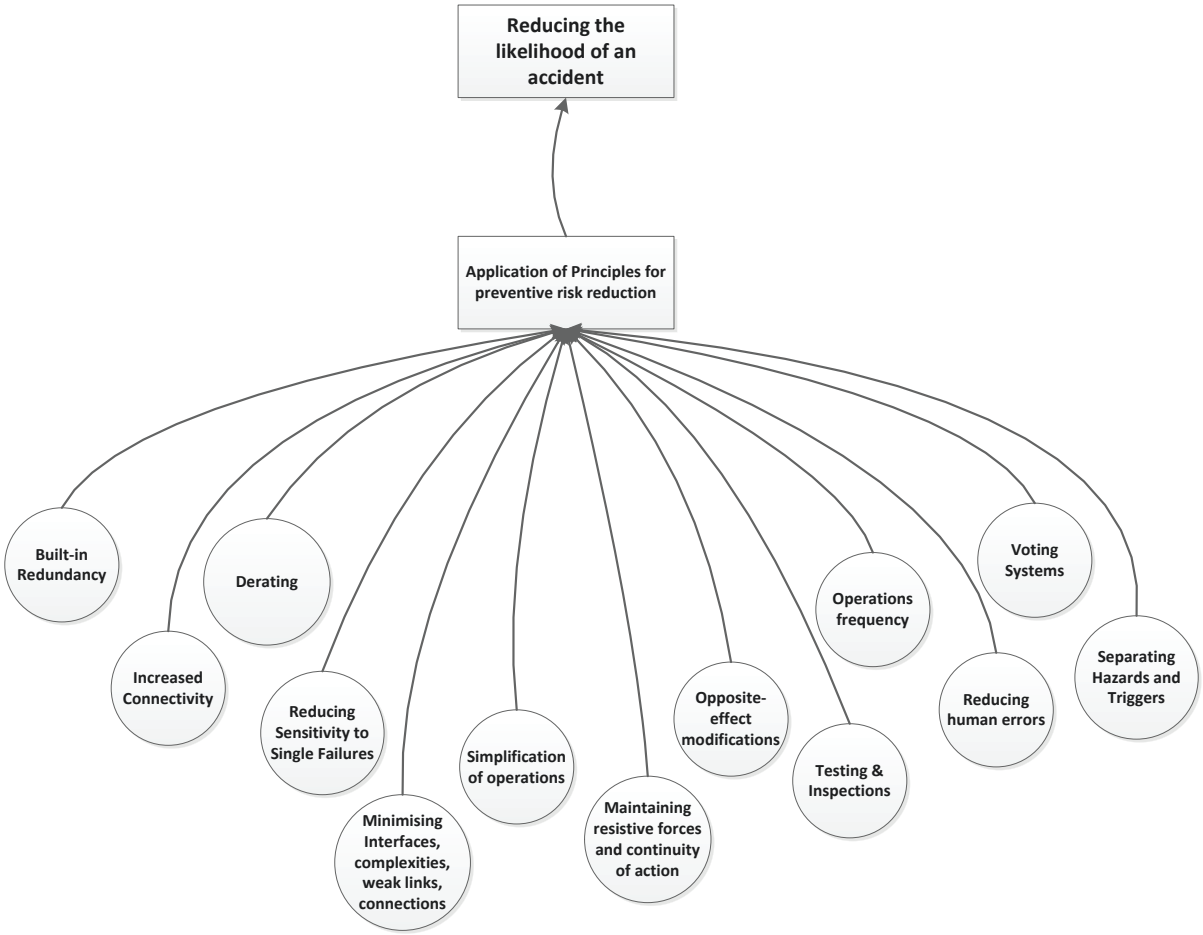


Figure 18: Generic principles for reducing the likelihood of an accident

The position established by the descriptive work in subsequent sections of Chapter 5 is that by demonstrating the implementation of these preventive principles in specific risk reduction applications, the decision-maker or safety analyst can easily identify and assure that measures selected will effectively achieve the risk reduction requirements (either as preventive or protective measures). Furthermore, a combination of this understanding with comprehensive studies on cost and magnitude of removed risk can adequately support and guide a selection process that also addresses constraints such as a fixed budget.

5.2.3 Typical Preventive Risk Reduction Systems

Operational risk reduction for customers and front line railway personnel is the primary consideration during the design, development and operation of railway systems. The inherent safe design philosophy is

applied using the same preventive risk reduction principles for the provision of safe operations. The railway risk reduction requirements ensure that safety systems introduced to operational railways for major train control and operations systems achieve the following functions:

- Perform train separation;
- Point and route locking with respect to train location;
- Platform and train door control;
- Fulfilment of requirements on train speed control and travel direction;

These primary railway operational risk reduction requirements are implemented with the use of safety-related systems on the trains, specified trackside locations, system control centres and at point interlocking locations. By incorporating ALARP principles, the risk reduction requirements also include that in the event of failures, the safety performance of the railways against agreed safety benchmarks is not compromised.

Train separation is achieved when the railway control system maintains an assigned 'Safety Distance' between all trains and obstacles. This is the distance between the commanded stopping point of a moving train and the confirmed position of the rear of the preceding train or obstacle, such as buffer stops and misaligned points. This distance is calculated and assigned allowing for worse case scenarios where the safe separation is still maintained.

The typical train control centre is responsible for the control and interlocking of all points. It receives status point from the point monitoring systems and performs the point interlock function based on the status, reservation and occupancy reports for the points. Once the train control centre receives communication of set and locked points in the correct position, a train can be cleared to move over the points and the stopping point for the moving train will also progress, as it is a moving target train stopping system.

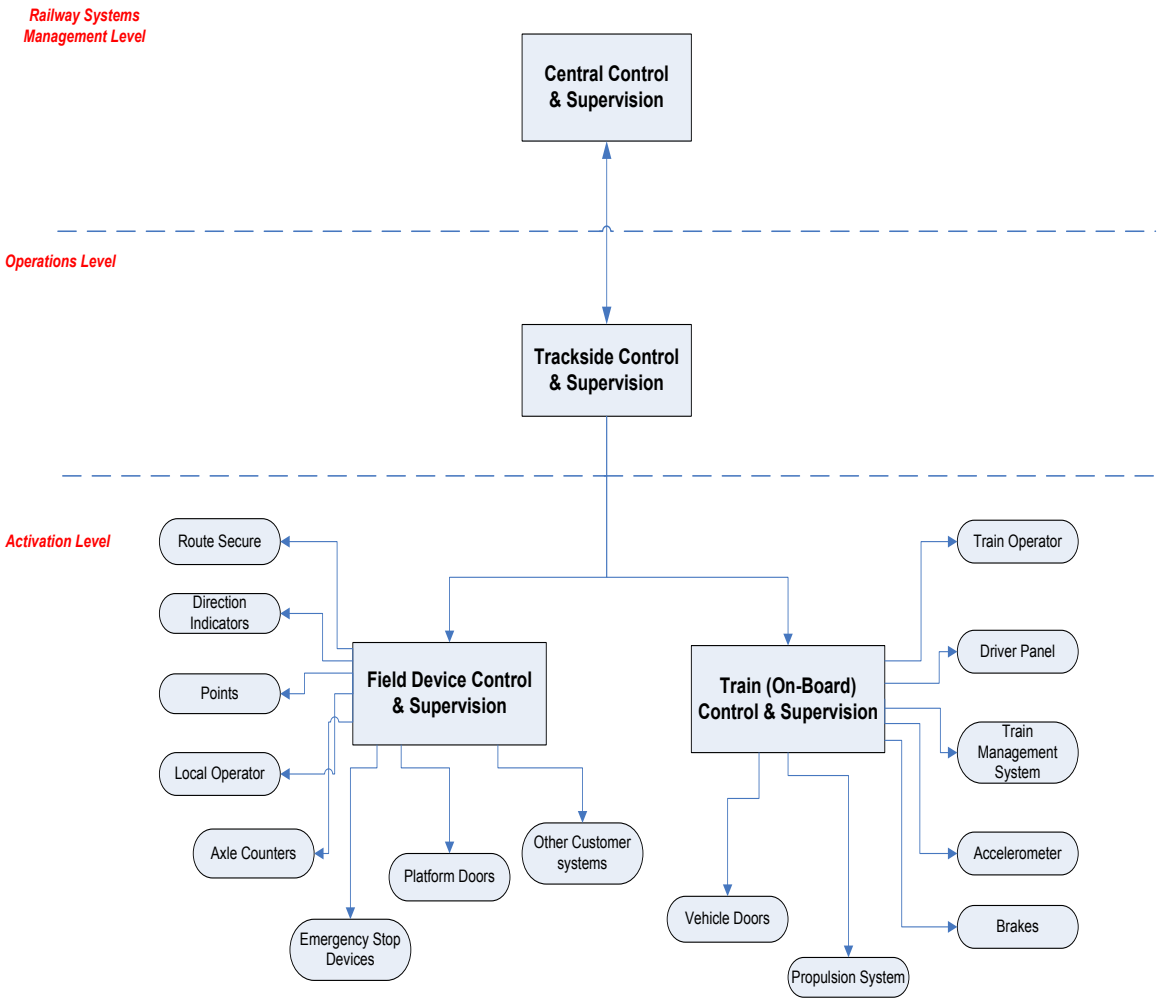


Figure 19: Railway Systems Levels of Control

Different railway infrastructure owners, operators and suppliers use diverse systems for these primary functions. However, an outline of subsystems used to achieve preventive logic risk reduction that further support the railway safety case is presented in Figure 19 above. Some of the fundamental systems include:

- **Axle counters** provide point dead locking and tracking of trains by counting the number of axles so that trains are detected and tracked as they enter or leave block sections, or guide-ways in the case of moving block systems.
- **APR (Absolute Position Reference) Transponders** are passive devices located between the running rails or track used by the train as an absolute position locator.
- **ATC** means Automatic Train Control which comprises the Automatic Train Protection (ATP) and Automatic Train Operation (ATO)

- **ATO** is the Automatic Train Operation system, a subsystem of the ATC as defined above. In normal operation, the ATO system is responsible for automatic driving of trains.
- **ATP** denotes the Automatic Train Protection system, a subsystem of the ATC. The ATP ensures that the train does not exceed the enforced or stipulated movements and distances between trains. Proper application of the ATP must take speed restrictions into account with the design objective based on the fail-safe principles in accordance with railway risk reduction requirements.
- **Position detectors** are trackside devices used to detect a train wheel to give an indication of the train or vehicle position within sections of the railway network. This provides information on the state of occupancy (i.e. occupied, clear or undefined) to the signalling system.
- **A track circuit block system** consists of block signals, non-block signals, overlaps, signal sections and track circuits. A track circuit is a section of a railway line with fixed boundaries providing information on its state of occupancy to the signalling system. The overlap within a track circuit block system is the distance ahead of a stop signal up to which the line must be clear or locked for the following signal to clear for train movement.
- **Train Protection and Warning System (TPWS)** is a safety system that automatically applies a train's brakes if it approaches a signal too fast, or if it fails to stop at a signal set to danger.
- **Trainstops** are devices, controlled by the signalling and only operate a trip-cock when a signal is passed at danger.
- **Trip-cock** is a device attached to the leading right hand positive shoe beam operated by an arm which, when pushed back by a train stop in the up position, causes the automatic operation of the train’s brakes.
- **Correct Side Door Enable** is used to inhibit the release or opening of train doors if the doors are on the wrong side or the non-platform side to prevent passengers falling onto the track. This function is normally included in the specifications for selective door operation capability.
- **Selective Door Operation** is used for selectively opening of power doors and the inhibition of other doors. This can be undertaken manually or via the use of automatic door selection devices. This is particularly used when a train extends over a shorter platform for passengers to safely disembark

- **Point System** (or Point Machines) in some applications, are all electric with integral lock and independent lock and switch blade detection used for operating railway turnouts. Some applications use electro-hydraulic point drive units.

- **Train arrestors are** devices designed to decelerate a slow moving train to minimise injury to staff and customers or damage to the train overrunning the correct stopping position at a terminal

- **The standard brake systems** used in railway applications are fail-safe designs. Most brake systems use compressed air, known as air brakes. When acted on, the compressed air pressurises blocks on wheels or pads on discs to initiate train-braking action. Electro-pneumatic brake control systems are digital control systems with fail-safe features only used on multiple unit trains. The fail-safe feature is energised to release and de-energised to brake. The digital control system for braking eliminates the need for a brake pipe typical of pneumatic systems.

- **Wheel-slip/Wheel-slide Protection system (WSP)** is a train system for detection and rectification of wheel slip during authorised movement and skids during braking.

Other systems, processes and applications are defined in the following sections. In addition, assessment of the risk reduction measures, and the attributes and capabilities for reducing the likelihood of accidents are further highlighted. This exercise is required for understanding the applications and application strengths of the risk reduction measures prior to use in cost effectiveness studies which support the selection of risk reduction measures.

5.3 Application of Preventive Risk Reduction Principles

The preventive risk reduction principles outlined in 5.2.2 are essentially those that provide guidance to the effective use of the measures. By clearly mapping the measure to be selected to the corresponding principle, insight into each measure's preventive properties (limitations or strengths) for specific risk reduction applications is determined. Subsequently, the comprehensive understanding of the limitations or strengths of the preventive measure within the application generates requirements for introducing additional or supplementary measures. This is particularly useful when a large number of measures or combinations of measures are considered for a given set of risks. A good example of its effectiveness is provided in the assessment for the introduction of axle counters (Weli and Todinov, 2013a).

5.3.1 Built-in Redundancy

Built-in redundancy is an effective design feature targeted at the prevention of failures and consequently major accidents on the railways. Its use in railway application, though effective, also results in design complexities which increase the risk of failures. Built-in redundancy as a preventive risk reduction

principle is most effective when there are no common causes simultaneously degrading the redundant components. The benefits of built-in redundancy for major accidents are primarily:

- Increasing reliability and reducing the frequency of accidents (safety)
- Increasing the operational time (increasing the system availability)

The general concept for developing fault-tolerant fail-safe systems for railway signalling systems is outlined in Chakraborty (2009). Design-related failures require a different strategy for the effective implementation of the options with built-in redundant features. The implementation of a robust quality management system enhances a fault-free design helping ensure that the redundant system is effective and achieves its risk reduction objective. Employing redundancy enhances the fault tolerance of the systems by eliminating single point failures. The built-in redundancy feature of the renewal of brake valve systems is effective for managing random failures leading to an accident such as collision between trains.

Several applications of 'built-in redundancy' on the railways as preventive measures can be associated with design options for risk reduction. These include:

- Brake systems and subsystems such as automatic braking systems, brake valves, controllers, failure detection and alarms
- Route locking systems
- Position detection systems such as track circuits and axle counters
- Train door units
- Power supply units
- Radio, communications and control systems

The use of this risk-reduction principle makes requires a thorough assessment to be undertaken on its benefits in specific risk reduction applications. An example of the need to assess the suitability of this feature is obvious in the use of redundancy in the design of points on railway networks. Point systems failures represent single critical points of failure on railway networks and are major contributors to accident risks such as collision, derailments, delays and cancellations.

The REPOINT Project (Bemment et al. 2012) investigated the potential benefits of redesigning points and incorporating redundancy methods that are used in other safety critical industries such as aviation. . Building additional redundancy in existing point systems is potentially cost intensive without resulting in a proportionate risk reduction benefit. The study shows that the effectiveness of built-in redundancy to reduce the risks associated with points failure is achieved with changes to operating rules. The

application of 'built-in redundancy' through physical re-designs and installation of new railway lines as a preventive risk reduction measure may not be effective (disproportionately expensive compared to benefit). This study illustrates a typical example where built-in redundancy can provide the cost effective solution through unconventional means (i.e. operating procedure/rules).

5.3.2 Increased Connectivity (Networks and Operations)

The risk of failure of a system used for safe applications on the railway is significantly reduced when cross-links are introduced in the design. Introducing cross links in reliability network reduces the sensitivity to failure of single links thereby reducing the risk of system failure. For example, a mesh-like network is less sensitive to failure of a single link compared to a tree-like network. A single failure of a link in tree-like network causes the communication with the system after the failed link to be lost. The communications in a mesh-type network are retained event after several simultaneous link failures.

Several topologies are used in signalling and control networks for railway systems development and applications, to enhance reliability and safety functionality. These include their use in track circuit signal devices, passenger information systems, video surveillance, position detection and on-board train units. The basic topologies are:

- Point-to-point network designs
- Point-to-point with fault tolerance (additional channels for safety and reliability)
- Star network designs
- Ring structure network designs resulting in increased redundancy using optical connections
- Compressed ring structure i.e. Ring in linear network design
- Mesh structures
- Chain with bridged taps
- Ring structure (increased redundancy using a backbone network)

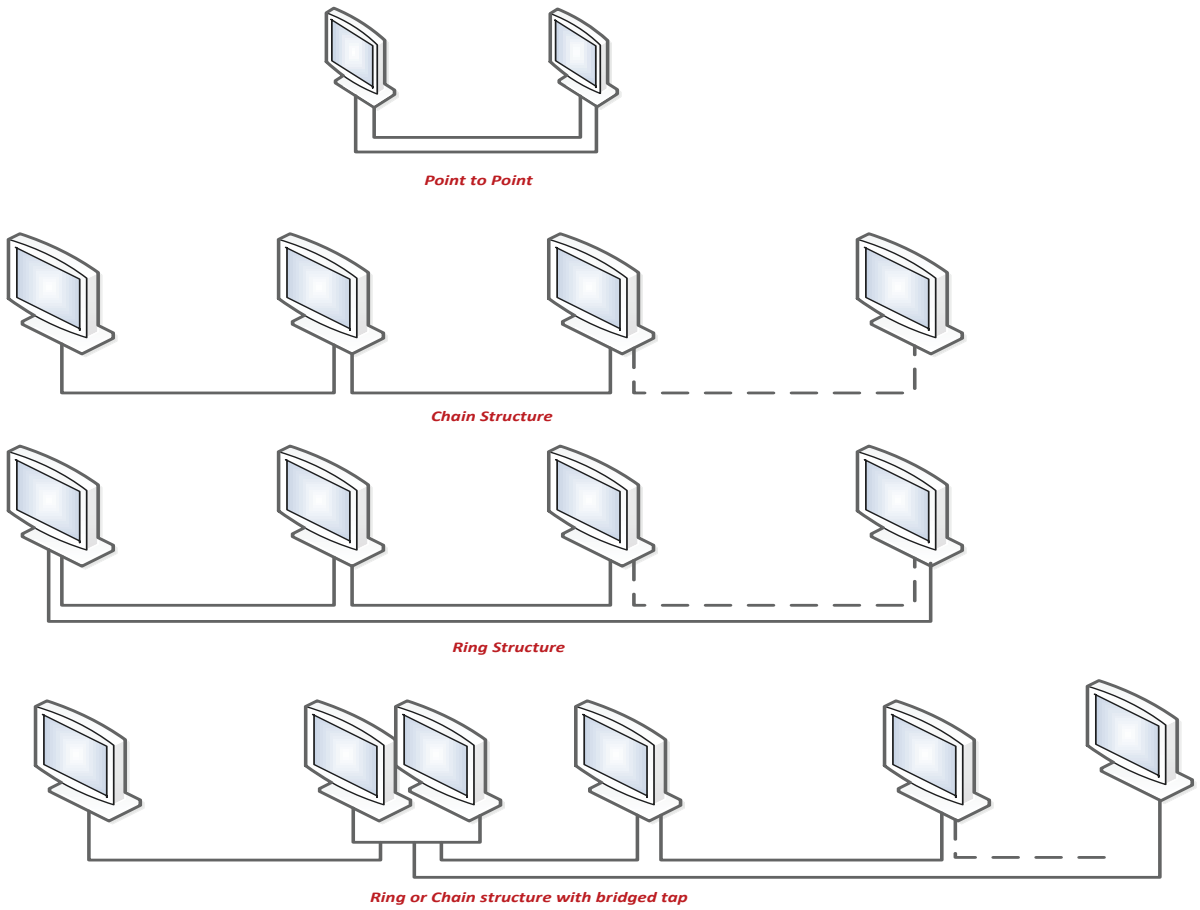


Figure 20: Network topologies used on railway control systems

Designing with modularity and configurability in mind is vital to cost and risk reduction. To accommodate these network designs with performance and safety benefits, developments of safety critical systems are progressing towards Ethernet/IP-based network structures rather than serial transmission networks (point-to-point networks).

These different topologies come at varying product lifecycle costs. The effectiveness of the designs can only be determined on application to specific risk reduction cases. However, the assured reliability and availability of a robust network, insensitive to failures of individual links, must drive implementation decisions especially in cases where delay and safety costs far outweigh design and implementation costs.

Another effective use of connectivity principle is its capability to facilitate the design and implementation of timetables to address emergency situations such as degraded mode operations and subsequent accident prevention. This application of the principle is essential for effective risk reduction. The implementation of timetable simulation tools for safety and performance modelling provides forecasts of failures, delays and accidents. Essential features within these tools include:

- Train length;
- Passenger connections;
- Stabling points or depots;
- First and last dwelling points and time;
- Peak and off-peak times;
- Forecasted lost customer hours with predicted system failures/failure rates;
- Expected passenger loadings.

Improved connectivity supplies fast information where it is needed for quick design of emergency timetables, which in turn reduce the possibility for overcrowding. Reduced overcrowding of platforms reduces significantly the likelihood of train platform accidents. Adoption of the principle of connectivity of systems and networks for railway designs prior to major railway projects greatly reduces the risk of disruption of the railway service.

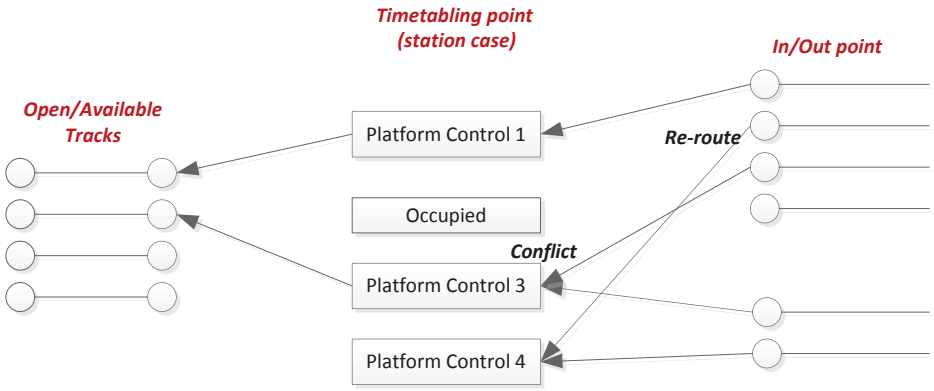


Figure 21: Simplified connectivity of timetabling points on a train network

5.3.3 Voting System / Technology

Voting systems on the railways are significantly applied on trackside systems by the use of complex microprocessors. Railway interlocking systems for safe train operation are typical examples. The interlocking systems control the signals and switches on a railway line.

A risk reduction measure incorporating a voting system can be used to significantly reduce the probability of an accident by eliminating operator's error. The fundamental functionality of voting is based on replicating the initial component *A* to *n* identical and independent components, each of which receives the same input as the original component. The output of the voting system is usually determined by a majority vote of the independent signals. Even though the individual component may be associated with a significant probability of an error, the voting system reduces by orders of magnitude the probability of a

n erroneous output. This significant reduction of the probability of erroneous output (system error) significantly improves safety and reliability.

The voting features for risk reduction are found in complex systems such as axle counters, on-board processors for train control, and field element controllers. These systems in risk reduction applications are nominally developed to the highest safety integrity levels. Figure 22 provides three controls software platform architecture variants for generic train control systems to achieve required risk reduction.

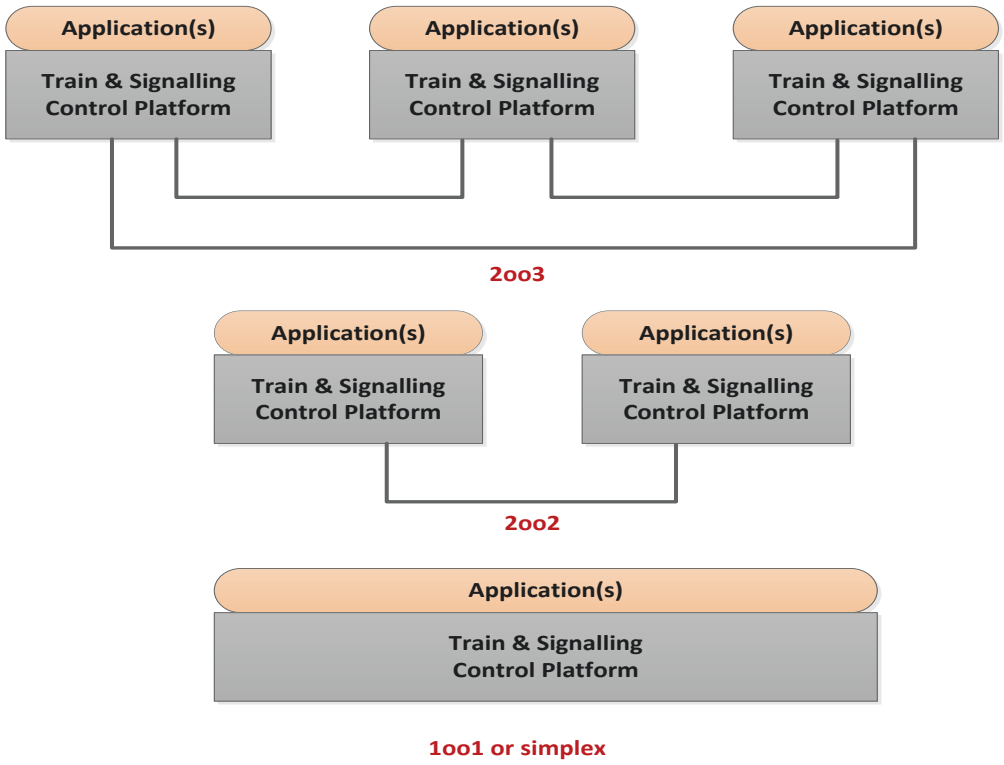


Figure 22: Software platform architectures used for railway safety systems

The two-out-of-three (2oo3) architecture provides a configuration for the core controls platform. This is employed for high integrity safety applications to achieve both safety and fault-tolerance requirements by, using the majority-voting feature to effectively reduce the probability of failures. The 2oo2 architecture provides a lower level of safety, however a reduced low nuisance trip rate. The 1oo1 configuration is used for safe operation on a single channel with diversity within the controls subsystems.

5.3.4 Reducing Sensitivity to single failures (Systems and Operations)

Sensitivity to failure of single systems or the potential effect of single operational failures is a weakness in railway applications. They also result in a chain of failures (i.e. domino-effect) and ultimately lead to major catastrophes such as railway accidents. Common methodologies employed in the railway industry to tackle sensitive designs include:

- Introducing design redundancy in train control and signalling systems for reducing single failures which can cascade into catastrophic accidents

- Robust isolation, screening, filtering, earthing, segregation, detection and fail-safe techniques against electromagnetic interference. A 'block/section clear signal' is the result of a single system failure such as disturbance effects on line-side telecommunications or electronic circuits potentially cascading to an operational failure or accident. Hill (1997) illustrates the vulnerability of railway systems to electromagnetic interference. Mauriello and Clarke (1983) also provide predictions for severe levels of train electromagnetic interference resulting in degraded operations.

- Reducing design and operational safety functionality that heavily relies on a sequence of operations and human interference to meet its overall risk reduction objective: e.g. Signal passed at danger (SPAD) incidents that may lead to accidents.

On some railway networks, a SPAD incident currently requires a sequence of actions to make the railway safe. These actions introduce significant system and human risks of failure. A thorough review of several studies on SPAD brings to light some noteworthy views on the effectiveness of proposed and current solutions to SPAD. Evans (1996) outlines how the introduction of Automatic Train Protection (ATP) systems reduces the risks associated with SPADs. However the cost of implementation far outweighs its benefit. Davies (2000) supports this and argues that despite the relatively high frequency of SPADs, less that 1% of SPAD incidents result in accidents. His study also proposes that the best solution to SPAD related incidents is to fit the Train Protection and Warning System (TPWS) at only the highest areas of risk within the network, rather than the European Railway Train Management System /European Train Control System (ETCS), which is a form of automatic train protection.

A similar, yet different principle is "reducing the sensitivity to common cause failures". A common cause failure (CCF) is the simultaneous malfunction of several elements of the system or operation triggered by a single source. Unlike the single failures, CCF cannot be addressed by redundancy. Where redundant control systems are vulnerable to CCF, system diversity is applied as an effective means of reducing risks from common cause failures. Li et al (2013) considers the common cause failure of train rear-end collision accident using fault tree analysis. The result of the study shows the significant influence of CCF on the system reliability. The minimal use of diversity in safety-critical industries appears to be driven by reliance on high-quality practices and procedures, nature of the applications and behaviour of the processes, implementation constraints such as cost and acceptability of risk (Wood, 2010).

An example of the effective application of system diversity through diverse programming for railway interlocking systems is described by Dumus et al (2011).

5.3.5 De-rating

De-rating is widely employed to reduce the level of operational stress significantly below its nominal value. This is achieved by limiting the stress (electrical, mechanical, thermal) on railway systems exposed to temperature and operating extremes. Derating is a form of design safety that has applications in railway safety-critical systems such as track de-stressing, temperature adjustments on train detector devices, conductor rail power adjustments and safety design adjustments due to vibration, shock and environmental constraints. Its application is generally in cases where there are uncertainties regarding the variation in strength and load. It can be effectively used to reduce the risk of failure of railway safety systems.

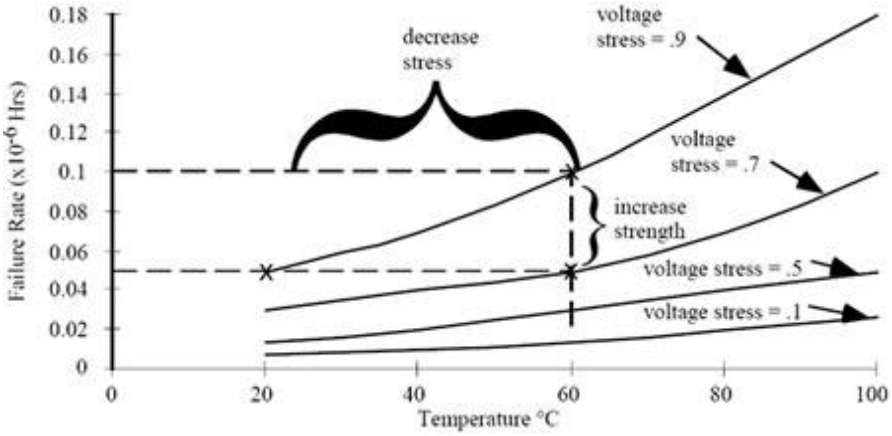


Figure 23: Example of stress failure analysis for an electronic component – illustration of stress and strength de-rating

De-rating as a preventive risk reduction feature on railway safety systems can be identified in basic applications such as managing temperature effects that lead to voltage imbalance in track circuits and position detection systems. Shaofeng Lu (2011) illustrates the use of derating in 3kV DC railway current source inverters and for speed control of AC motors in railway traction systems.

5.3.6 Simplifying Railway Safety Systems or Operations

Simplifying systems and operations can be effectively achieved on the railways by reducing:

- The number of systems or operations used in safety related actions
- The systems and operational interfaces
- Separation of safety-critical and not safety-critical systems or operations

The simplification of systems and operational functionality of risk reduction measures is frequently seen in the use of software-based systems to simplify safety application requirements. Examples include:

- Electro-pneumatic braking systems with with fewer components and simplified control 'fail-safe' systems, to enhance braking performance,
- Use of moving block systems (usually level-3 ATP), substantially reducing the number of systems required such as line-side signals, train stops or manual (driver) interventions.

The adoption of this principle significantly reduces bulky, complex designs and correspondingly, the failures associated with the complex designs and overloading of systems and railway operations. The introduction of new technologies as outlined does not preclude the use of other risk reduction measures to supplement safe operations of the railway. The introduction of such systems will bring specific risks, which also require safe failure isolation techniques, working rules and procedures with adequate administrative controls to ensure their effective implementation.

Other potentially overlooked applications of this preventive risk reduction principle are the introduction of new trains with improved seat designs to minimise passenger injuries, the simplification of platform and station area designs for effective security (passenger safety) and crowd control, and possibility for introducing more signals and warnings.

5.3.7 Reducing Weak Links, Connections and Interfaces in Systems or Operations

A high number of interfaces and connections invariably results in weak links in railway system designs and operations. The move towards the introduction of communication-based train control systems as a solution in the conventional fixed block system does have its challenges. At the system level, the primary risk of radio-based moving block systems is communications loss. This loss or failure can be a result of component (subsystem) malfunctions, weak signal strength, electromagnetic interference or overloading of the vital communications unit. Such failure does result in emergency braking. The increased frequency of such events leads to service delays and risk of collision.

In practice, increasing the number of transponders, induction loops or line-side communications units addresses most cases of weak signal strength due to bandwidth limitations. Another reliable solution in areas such as tunnels is the use of leaky feeder cables. The effectiveness of the leaky feeder cables as a solution for tunnel radio-based transmission systems has to be balanced against the material, installation and maintenance costs.

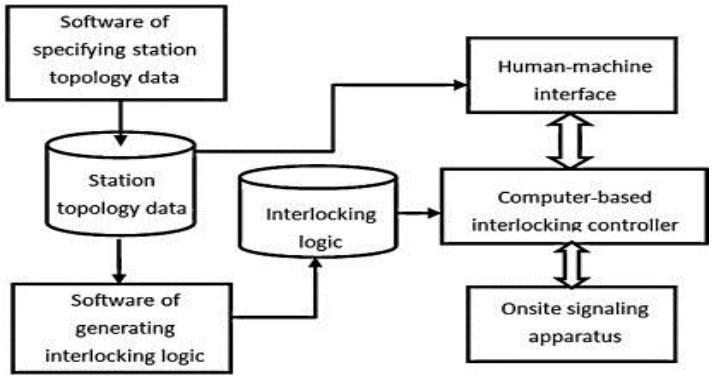


Figure 24: Use of open communications systems and cyber attack

An interlocking software system consists of four parts. These are the tools that specify

- Station topology data
- Generating the interlocking logic
- The supervising software that runs on the human–machine interface
- The executive software runs on the computer-based interlocking controller.

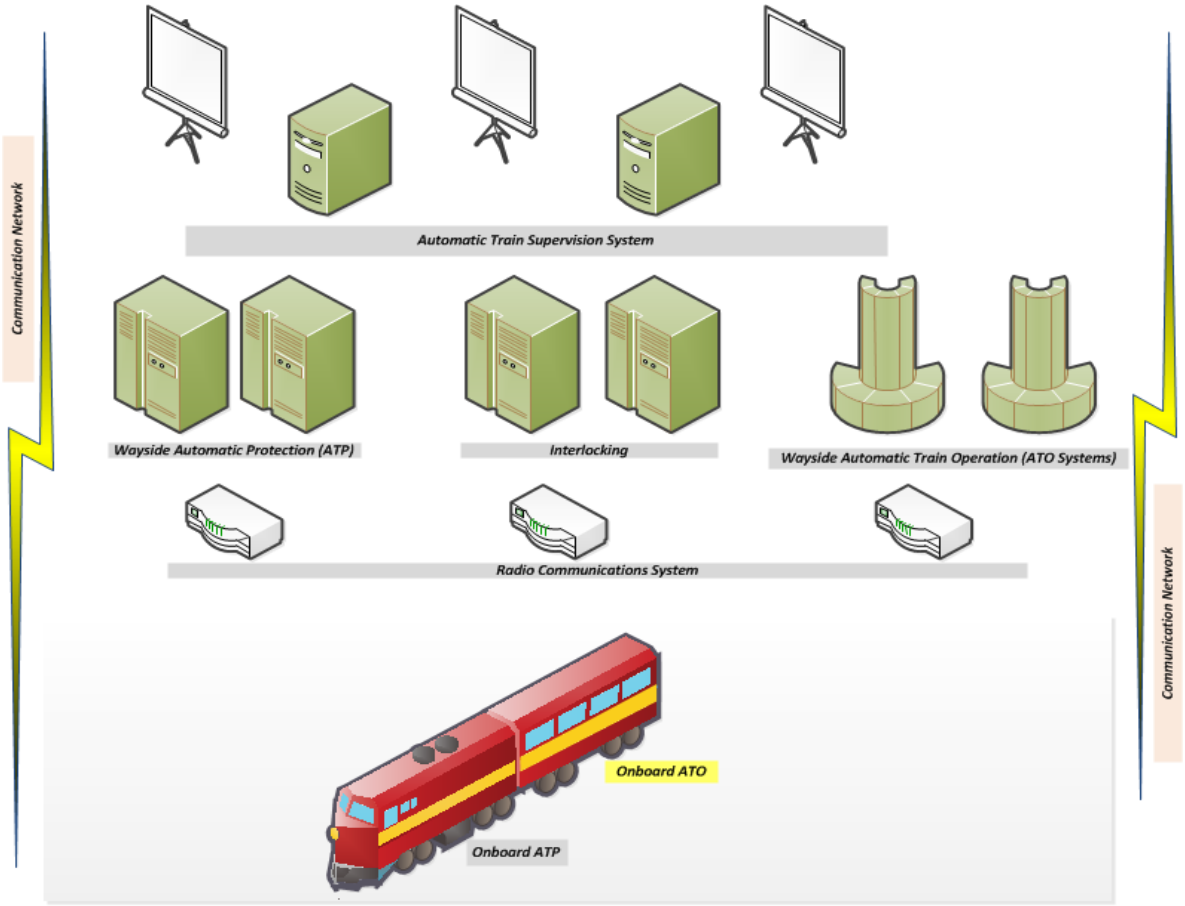


Figure 25: Generic Communications based train control system architecture

Train control systems that employ open standards for wireless communications are subject to communications network intrusions and hacking due to the vulnerabilities associated with open networks. The greatest risk from these issues on safety critical equipment is the increased likelihood of a safety hazard. Effective risk reduction is achieved by additional defensive techniques, which mitigate against attacks using reliable security controls for safety applications.

Systems design and architecture that can reduce weak links in railway control systems that are used for safe railway functionalities is published in Druschel et al (1993); Kreitz et al. (1998). Liu et al. (1999) illustrate how correct protocol stacks can be configured from Ensemble's micro-protocol components, and how the performance of the resulting system can be significantly improved. In Paleska et al. (2012), a threat analysis is performed, identifying both safety and security hazards that may be common to all model-based development paradigms for safety-critical railway control systems, or specific to the openETCS approach. In the original rationale for the openETCS initiative, Hase (2011) relates security issues observed in standard software products directly to threats expected in ETCS developments. For example, the paper argues that if backdoors could be integrated into standard commercial closed source products, the same could happen to railway control systems software.

5.3.7.1 Compatibility and Interoperability

Significant interface challenges with implementing radio-based train control systems (especially as a layer on existing conventional systems with future migration plans) are compatibility and interoperability. This is also a significant issue in complex railway systems where different operators with different train control systems cross paths. The validation activity to demonstrate that this weak link has been designed out is heavily weighted on extensive migration and pre-operational testing. Ebrecht and Meyer zu Hörste (2012) use existing test methods to prove technical as well as operational interoperability. The stepwise integration of testing considers three layers for a communications-based train control system:

- Testing to validate conformity of a single component – the on-board unit (OBU) of the European Rail Traffic Management System (ERTMS).
- Integration test for assemblies, the complete on-board equipment.
- Tests for the validation of operational serviceability.

5.3.8 Maintaining Continuity of Action and Resistive Forces

Maintaining the continuity of motion and capability to stop a train in an emergency (on demand, including maintaining stopping/parking) are two primary requirements of railway operations (Section 5.2.1). This principle is demonstrated by the wheel-slip and wheel-slide applications. Typically, specifications clearly state that a wheel/rail adhesion greater than 0.15 at any axle is required to permit the axle to rotate rather than slide. Adhesion failures contribute to a significant amount of railway

incidents including platform overruns, SPADs, collisions and derailment accidents. Examples of adhesion risk reduction measures with this preventive measure include:

- Vegetation management
- Fitting of wheel slip protection or adhesion improvers (wheel-slip and wheel-slide protection system – WSP)
- On-board sanding and fitted sander (service brake failure)

In most railway operations, integration of all three risk-reducing measures is employed for optimising adhesion. In order to achieve the greatest benefit from adhesion management systems for risk reduction, there needs to be an integration of the friction coefficient with the wheel-rail management system such as grinding schedules used in wheel and rail maintenance. Other primary considerations for effective risk management are materials, dynamics, friction, and application environment. Figure 26 presents the factors and interactions that influence adhesion management.

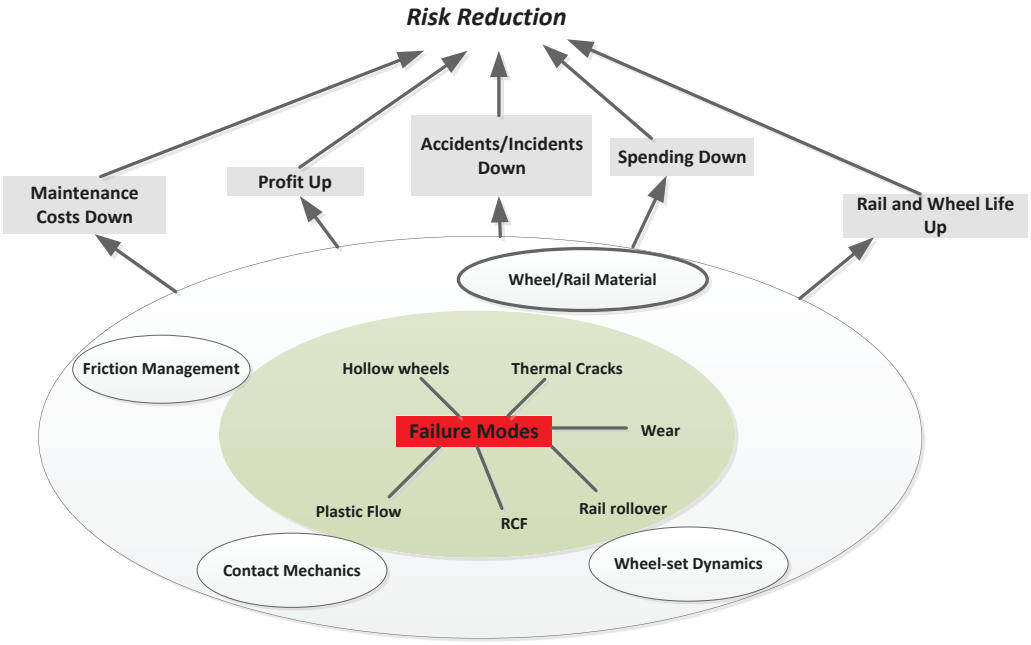
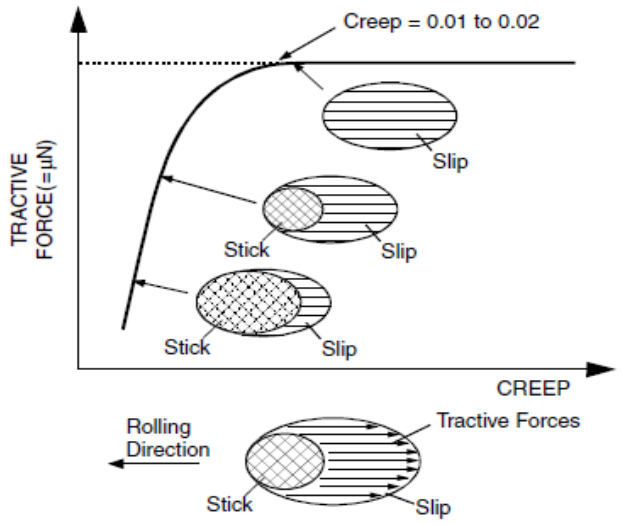


Figure 26: Adhesion risk management



Relationship between traction and creep in the wheel–rail contact.

Figure 27: Wheel/Rail friction. Extracted from Lewis & Dwyer-Joyce (2006)

Figure 27 illustrates the contact area between a wheel and rail. The diagram highlights adhesion effects using slip and non-slip regions. With increased tractive force, the slip region increases and non-slip decreases leading to a rolling and sliding contact. At the saturation point, the non-slip is zero and the contact area is in complete slide mode. The curve can be influenced by application of adhesion risk reduction measures as outlined above or by lubricants (if desired) to control friction at the rail wheel interface.

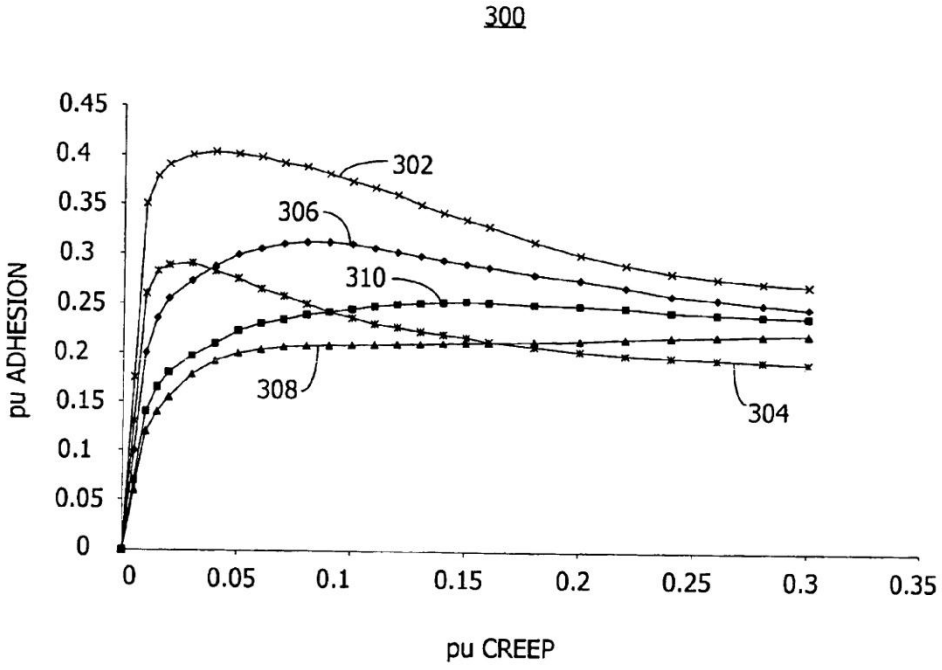


Figure 28: Adhesion/creep (railway train friction management) – extracted from Railway train friction management and control system and method http://www.freepatentsonline.com/6893058.html. 14-02-12.

Figure 28 is a further demonstration of the wheel slip and slide studies on railway train adhesion and provide fundamental guidance to decision makers on applications that support risk reduction:

- **300** – Illustrates a typical adhesion creep curve
- **302** – Adhesion characteristics of dry sand that provides the highest level of adhesion for each level of per unit creep
- **304** – Wet sand higher level of adhesion than dry rail
- **306** – Dry rail
- **308** – Oil/lubricant rail for applications where less friction is required. Provides the least adhesion level
- **310** – Adhesion curve for water. This also provides improved reduced adhesion when compared to dry rail.

For adhesion management schemes to work effectively, supplementary options or combinations of the following may be required for preventing accidents:

- testing the brakes (run extended brake tests to assess the adhesion condition),
- maintenance;
- training of drivers (including enhanced monitoring of sand hoppers);
- communications procedures for alerting control room/drivers of reduced adhesion conditions on the network or the particular line;
- train release procedures, braking procedures, use of redundant and reliable braking systems;
- inspection regimes for tracks (e.g. use of DVT vehicles);
- control system fitted to trains to prevent locking of wheels;
- improved prediction tools for accurate forecasting of the behaviour of a train in low adhesion conditions and tool must consider rail head conditioning;
- influence of sanding and simulations of more than one vehicle;
- signalling modifications such as extension of overlaps;
- operational restrictions such as restrictions on the use of specific high risk junctions, sharp gradients and level crossings.

5.3.9 Opposite-Effect Modifications (Introducing Modifications with Opposing Effects to Failure-Related Changes)

Speed restrictions are imposed at extreme temperatures as a result of high risk of buckling. However, this comes at a cost to the operator. The decisions made to enforce speed restrictions are to ensure passenger safety. Stressing of railway tracks is a good example of the application of forces to negate conditions that result in track buckling and potentially derailments. With high-speed derailments, there

is a significantly increased likelihood of subsequent loss of life, direct costs of compensation, repairs, and loss of business.

Rail de-stressing otherwise termed “track stressing” is used to reduce track buckling. Track buckling is caused by shrinking or expanding large sections of steel due to temperature variations. Track stressing as a preventive risk reduction measure is generally considered a cost effective way of reducing the need for speed restrictions, buckling and subsequently accidents. However, the cost of stressing a track results in disruptions, introduces additional welds and associated risks, heavy hydraulic tensioning equipment, welding equipment, and extensive labour including stressing engineers and welders. This cost can be minimised by developing and implementing logical condition monitoring strategies that can direct stressing effort to high risk areas especially in situations of financial and budget constraints.

Figure 29: Track buckling risk contributor to derailment accidents

Current risk management strategies for reducing the risk of rail buckling and associated failures incorporate inspections and track stressing for effective reduction of risk and invariably, cost. Risk-based inspections are used for monitoring and measuring the quality of sections of track. Static checks undertaken by track personnel in some cases use supersonic measuring devices and dynamic checks are mostly executed by special track condition monitoring trains. The use of monitoring vehicles depends on the frequency of use of the track section. This varies from the legal minimum of once per year to weekly checks for tracks used regularly.

The stress free temperature (SFT) of 27 degrees is the temperature at which tracks are installed in the UK. Chapman et al. (2008) maps the variability or rail temperature along different sections of track and

presents the UK railway guide for critical rail temperature values for standard track in different states based on overall track structure.

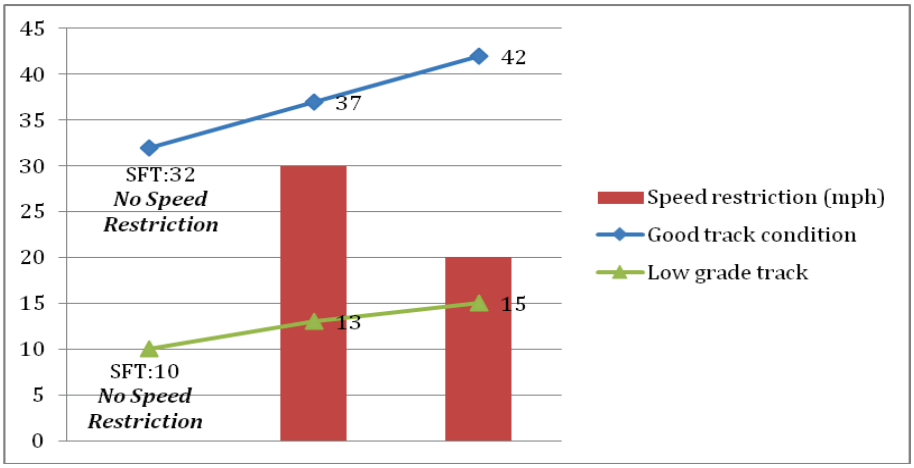


Figure 30: Speed Restrictions and Track Condition (adapted from Dobney et al, 2010)

The chart above indicates the reducing permitted speed imposed on the railways with increasing temperature for good and low-grade track conditions. Dobney et al (2010) suggests that an improvement in the quality of track, track-bed and subgrade is required for challenging temperature extremes in order to prevent the buckles and delays that could increase in cost by 800% over seventy years. This assessment only covers the cost of buckling and delays.

Relevant discipline leaders within track, signalling, operations and maintenance ensure the stressing of the track, track circuitry testing and track inspections are signed off and that a certificate is issued to confirm that the track is ready for operational use. This is an effective additional preventive risk-reduction measure as a means of establishing that the track is fit for operational use.

Other risk reduction measures that reduce derailments and effectively support the track stressing include training, speed restrictions, track alignments and refurbishment. For track stressing to be cost effective as well as to minimise the risk of buckling, a robust track inspection strategy must include:

- Use of more accurate systems such as train mounted equipment
- Follow-up with track walks in high risk areas
- Regular meetings between track-related disciplines
- Proactive programme of track refurbishment including track stressing

5.3.10 Operations Frequency

The frequency of train operations on a network can be used to prevent and attenuate the impact of accidents such as derailment or collisions. A practical example is the introduction into service of additional trains to reduce overcrowding.

Overcrowding potentially results in passenger crushing at the station or platform; train overcrowding resulting in movement accidents and platform/train interface accidents. This leads to further increased risks in the event of an accident, and potentially leads to health problems due to high temperatures and lack of ventilation.

Supplementary measures to support effective use of the operations frequency principle in this application (via increased train frequency) include station emergency and congestion plans, which set out the point at which the station is congested and the emergency procedures to follow. As part of the emergency and congestion planning, station staff are trained in crowd control procedures in the event that the station reaches its congestion limits. It goes without saying that operational changes (in this case increase of train frequency) can result in additional risks. However, such risks can be avoided by ensuring that an adequate level of emergency planning and training is implemented.

5.3.11 Testing (Revealing latent faults)

Railway safety systems are designed with high safety integrity levels as a result of customer and staff exposure to realisation of risks. To approve these systems for railway operations, a key requirement is that design safety features such as monitoring, diagnostics, alarms, trips (automatic or manual), and fail-safe must be demonstrated. These features address potential faults and the handling of the faults within the system. In addition, operational testing and proof tests are predominant requirements to ensure the safety system's integrity and its maintenance, so that it is not compromised by any latent faults.

Regular reliability tests on railway systems prior to operational use are safety case requirements. They aim to demonstrate and verify that claims for monitoring systems, diagnostics, alarms, trips, fail-safe systems with high integrity are accurate for the application/operational use. The aging of systems may contribute to increased risk of accidents if not properly addressed. Without a preventive objective and programme of testing (operations and maintenance), the effectiveness of measures such as emergency braking systems, trip-cocks and similar safety-critical systems is jeopardised.

Even risk reduction measures considered robust may be ineffective if they are not subject to regular tests. For example, in a real-life emergency situation, a train driver activated the correct side door enable system. However a spurious failure of the system resulted in all doors opening, exposing the passengers to falls, and additional risks from live conductor rails (electrocution) or being struck by trains running on the adjacent line. In emergencies such as these, details forgotten in planning or before operational use may result in additional or heightened risks. In theory, all trains have periodic testing programmed into the maintenance strategy. However; additional proof tests by the train driver (in this particular scenario) could have identified the faulty door system.

A reliance on carefully developed plans without a test strategy to support them is ineffective in most risk reduction cases. For example, an alarm plan may prove to be so complicated that in an actual crisis situation, it cannot be implemented correctly. This type of scenario could result in an accident, or significantly aggravate one. Complex cases of software reliability and assurance are particularly important considering the large amount of novel systems being introduced into the railway network. In order to reduce the likelihood of failures and the subsequent risk of system failures or accidents, self-developed systems and off-the-shelf software must also undergo testing before their operational use. Training of users of safety critical systems, including test teams, is essential for risk reduction and the realisation of the full benefit of testing.

Latent faults within a system or its operation are not always considered as relating only to physical systems: a totally different route is taken by experts in human factors.

Reason (1990, 1997) proposes that latent faults leading to accidents are in large part due to latent organisational conditions, effectively making the human error a 100% contributor to accidents and incidents. However, Young et al. (2004) whilst supportive of this factor throughout the accident sequence are critical of the insistence on identifying latent conditions, when active failures may have played a majority part. The above discussion naturally leads to the next section on human errors that require risk reduction measures.

5.3.12 Human Errors

HSE (2007) categorises human factors as environmental, organisational and work-related factors, together with individual characteristics. All or any of these may influence behaviour at work that can affect health and safety.

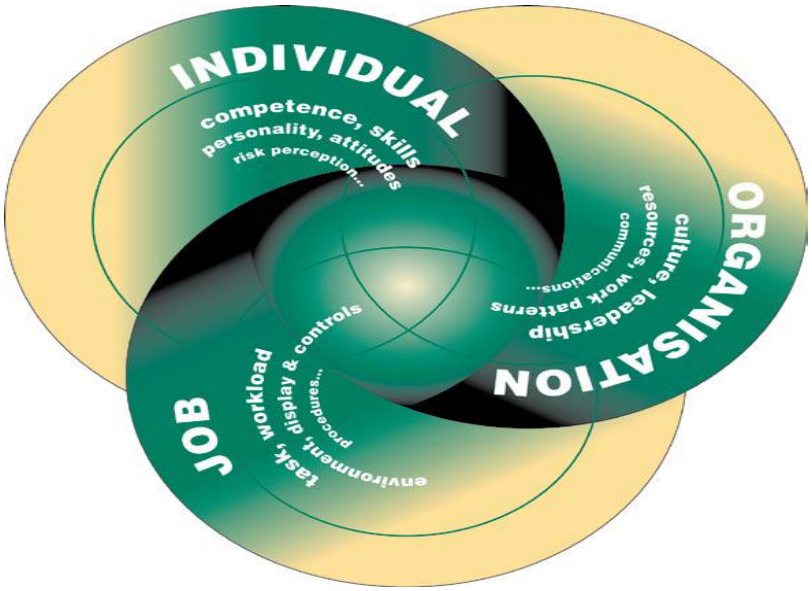


Figure 31: Human Factors (adapted from HSE 2007)

Human errors are identifiable in every aspect of railway operations from planning, statistical analysis, simulations and predictions, organisational structure, design, testing, manufacture, and maintenance. Practical examples include errors in activating braking systems, leading to collisions; failure of maintenance staff to adequately assess and hand over track before a first train, leading to derailment; or a passenger failing to note warning signs leading to sideswipe or platform-related accidents.

An increased likelihood of human error occurs in cases of a degraded mode of operation, where the safety of passenger and staff heavily depends on safety critical personnel such as train drivers, platform/station supervisors and line controllers. It is also important to note that for the effective prevention of risks due to human error, the passenger has a significant role to play in averting accidents. Indeed, very considerable percentage of passenger safety relies on the passengers. RSSB (2008) suggests that design is by far the cheapest and most effective way for a system or organisation to pay attention to or benefit from human factors. If a system delivers exactly the results required by an organisation, it represents a happy convergence of user requirements, designers' intentions and practical implementation.

With this consideration, a robust management strategy for risk reduction must ensure that less effort is directed at modifying human nature. Such attempts go down a long and costly road when the increased likelihood of resource turnover (e.g., constantly changing personnel undertaking specific tasks), is factored in. If design modifications are unavailable, an alternative and effective method is to improve and adapt working procedures and the environment. If combined with control measures determined by anticipating errors (risk assessments), results improve further. Figure 32 presents the key generic factors influencing the relationship between human performance and design for risk reduction.

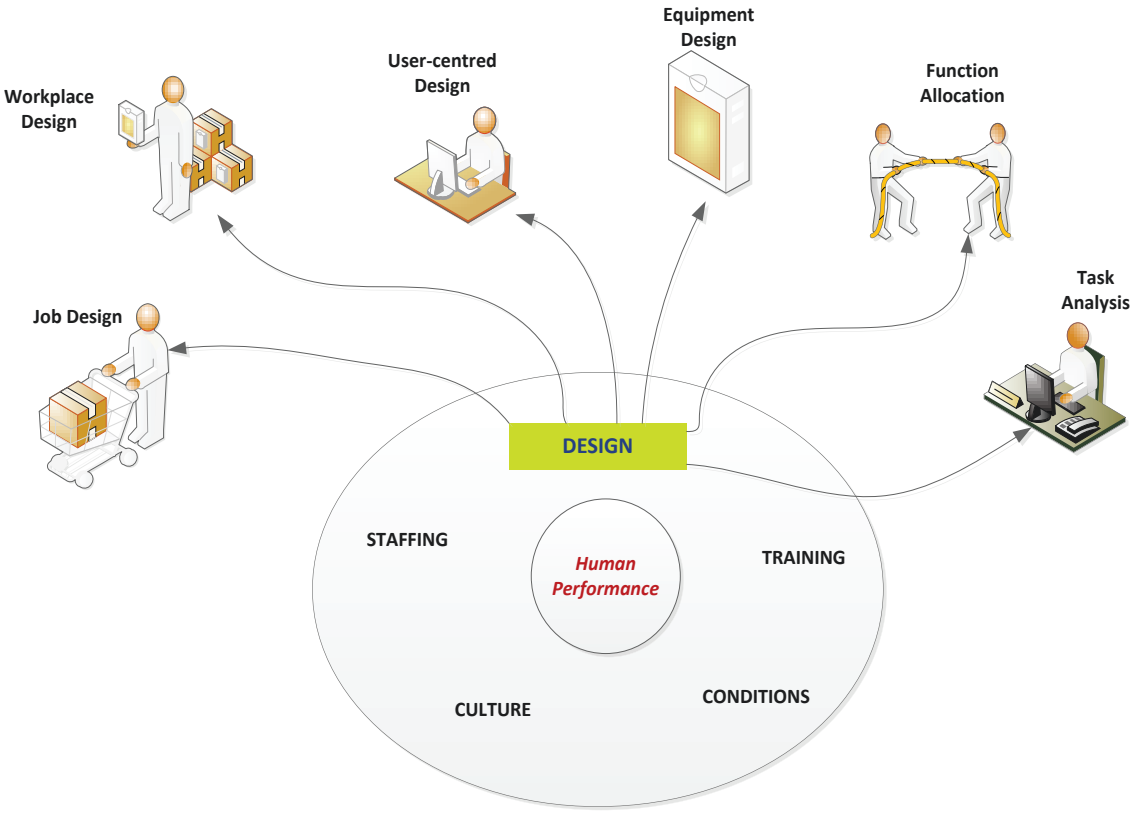


Figure 32: Design and Human Performance for risk reduction

The human error risk-reducing capabilities of generic systems are preventive as well as protective. These include:

- Interlocking systems
- Containment systems
- Surveillance systems
- Personal Protective Equipment
- Work Authorisation and Permits
- Self-Assessment methodologies
- Supervision
- Regulations
- Training

A lack of verifiable data and analysis has made the study of human factors on the railway fundamentally qualitative. The bulk of the analysis has been very comprehensive with its benefits. However, the CENELEC (European Committee for Electro-technical Standardization) standard EN 50129 requires the use of

quantitative risk analysis for determining Tolerable Hazard Rates (THR). Human error probability as a measure of human reliability is simply estimated as:

$$\text{HEP} = n/N \quad (5.1)$$

Where *n* is the number of observed errors and *N* the total number of actions undertaken.

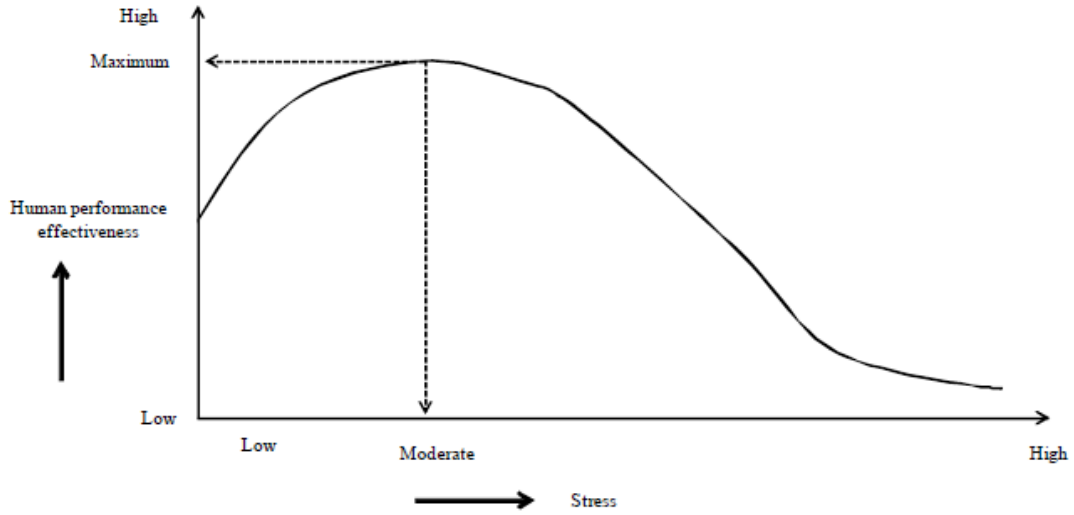


Figure 33: Human effectiveness versus stress curve (adapted from De Felice et al. (2011))

Human influence on the safe operation of the railways is a widely studied area; there are no publications that showcase measures with the desired preventive risk reduction attribute. The need to understand and highlight these attributes in existing and new measures is important in order to effectively utilise them in overall safety applications on the railways.

Baysari et al. (2008); Gaur (2005); Hickling (2007) provide comprehensive details in support of the argument that human error contributes to the majority of incidents in safety critical industries including railway operations. In their consideration of human errors as a contributor to 70% to 90% of transportation related accidents, De Felice et al. (2011) propose a 5-step methodological approach to improving railway transport system reliability based on Failure Modes Effects and Criticality Analysis (FMECA) and Human Reliability Analysis (HRA). Kumar and Sinha (2008) present a general theory of human errors, and stress the need to adopt optimisation in railway operations to the maximum possible extent and to develop a continuous monitoring system for the physical and psychological status of railway workers. Feldman et al. (2008) also present an approach to improve the determination of appropriate human error probabilities. Hockey and Carrigan (2003) argue that neither the railway industry nor the human factors field has advanced much, given the piecemeal and ad-hoc way in which safety problems have been approached. They regard this as a failure to develop a systematic strategy for

the contribution of human factors to safety research for railway operations. In a study based on distributed cognition principles, Busby and Hibberd (2004) reveal how organisational artefacts such as rules, practices and authority structures can be undermined, resulting in catastrophic failures of railway systems. The study reveals two patterns of failure: the first involves artefacts that support the kind of sense-making that people engage in. The second pattern is seen when the function of artefacts is undermined by the sense-making activity, or vice-versa.

Lenoir (1993) reviews safety critical operations of train dispatchers drawing parallels between cognitive processes in the behaviour of the dispatchers and the ways of working shown by test subjects in complex problem solving experiments. Lenoir discovered that dispatchers tend not to plan ahead as a result of railway network complexity and the frequency of change. The dispatchers' reactive method reduced the effectiveness of risk reduction measures and also highlighted the challenges of managing information flow within the railways, resulting in delays, inefficiency and accidents.

Van Welie and Van Der Veer (2003), Stanton et al (2005) and Kirwan (1992) all provide further insight into the functionalities and uses of standard human reliability methods such as Human Risk Assessment (HRA), and Technique for Human Error Rate Prediction (THERP). Results from these techniques are used as input in Quantitative Risk Assessments (QRA). However, their use on the railways for quantifying human reliability are fundamentally flawed as they focus on quantification for performance success and failure, and pay less attention to in-depth causes of observable human behaviour. These techniques do not consider cognitive processes in this area and are therefore unable to appropriately evaluate the triggers in human negligence or misconduct that result in accidents.

Baysari et al. (2008) considers frequent errors causing rail accidents and notes that accurate identification can lead to the development of appropriate prevention and/or mitigation strategies. Two tools for error identification were reviewed. The Human Factors Analysis and Classification System (HFACS) analysis indicated that lapses of attention (i.e. 'skill-based errors') were the most common 'unsafe acts' with drivers. The Technique for Retrospective Analysis of Cognitive Errors (TRACEr-rail) analysis indicated that most 'train driving errors' were 'violations' while most 'train stopping errors' were 'errors of perception'. Both tools identified the underlying factors, with the major causes of driver error to be:

- Decreased alertness and
- Incorrect driver expectations/assumptions about upcoming information.

Overall, both tools proved useful in categorising driver errors from existing investigation reports. However, each tool appeared to neglect some important and differing factors associated with error occurrence. Both tools were found to possess only moderate inter-rated reliability. The reviewers

recommended that the tools be modified, or a new tool be developed, for complete and consistent error classification.

RSSB (2008) acts as a guide for understanding human factors affecting the railway industry and provides a poignant example associated with use of the 'Automatic Warning System'. This is installed on all passenger trains in the UK, and exemplifies a system that was not designed with the limitations of human attentiveness in mind. It is a device fitted in the train cab, based on the now obsolete mechanical system of signalling that used to indicate either STOP or PROCEED. It sounds a bell when a clear (green) signal is passed or a buzzer when caution or danger is signalled. The AWS is a useful safety system when the press of a button does not acknowledge the buzzer, for then the train begins to stop automatically. However, times have changed since it was designed. With today's heavy commuter traffic, most signals will be at the 'caution' aspect, and given the frequency of signals (spaced 1km apart), most drivers will face two signals per minute. Since people 'automate' highly repetitive behaviour, drivers may lose focus on the need for carrying out this repetitive task, and act by reflex whenever the buzzer sounds. The end result is that drivers often hear the buzzer and press the button automatically without thinking about train speed and location.

5.3.13 Separating of Hazards and Triggers

Platform Edge Doors (PEDs) are used to isolate passengers on a platform from the track and is a very effective measure for reducing the frequency of platform-related accidents. PEDs can be effectively used to establish a 'protected platform area' and are effective for protecting against the escalation of platform incidents such as track fires. In most risk analysis and cost effectiveness studies, this last type of event is frequently neglected, resulting in the inaccurate selection of measures for reducing such platform-related incidents. PEDs are essentially dual as they are also largely applied to the preventive risk reduction of grave incidents such as suicides and murders, or when passengers fall onto the track, and for reducing the risk of accidents when trains are passing through a station at high speeds. PEDs are expensive measures and have rarely been considered on platforms until recently. To enhance the application of knowledge and thus cost effective implementations, the protective attributes, i.e. the benefits and effectiveness of PEDs for risk reduction, must be understood. To this end, these are more fully explored in subsequent sections of this chapter.

The train movement authority as another example of separating a train from another moving train is used to enforce a minimum distance between trains via the train control system. This method of preventive risk reduction through automatic train control systems ensures safety as well as improved train availability as more trains are permitted to run on the network

The signal overlaps, flank protection and trapping are designed into the railway network to control the risk of collision between an authorised train movement and a signal passed at danger movement. The signal overlaps are distances beyond a stop signal which must be clear or locked before the stop signal preceding the signal being passed can display a proceed aspect. The signal overlap is calculated and designed into the railway network to avoid the areas of conflict. The a areas of conflict in basic terms are the hazards i.e. the section of the railway line ahead of a signal at danger on which a head-on collision, same direction converging collision with another legitimately positioned train (moving or stationary) could occur in the event that of a SPAD. The flank protection separates or redirects a moving train (the hazard or trigger to an accident) from a route or overlap that has been set for an authorised train movement. Trap points are preventive risk reduction measures built into the exits from converging lines to derail an unauthorised train movement making train movement on adjacent running lines safe to continue operations. The Ladbroke Grove rail crash was a direct consequence of the failure of effective use of the signalling system complete with signal overlaps. The debate on the cost effectiveness of the signalling system at the time of the crash against the introduction of Automatic Train Protection systems (Automatic Train Operation and Control) was as a result of the mismatch between public opinion and the results of the ATP cost-benefit analysis. This accident, ensuing debates and inquiry was discussed in detail in Chapters 2 and 3.

5.4 Removed Risk Associated with the Separate Preventive Methods

From an extensive study of some UK internal organisation's operational risk assessments and safety cases, a selection of the risk contributors with the most impact on the railway risk profile is presented in this section. The different risk reduction measures evaluated for Derailment, Collision between Trains and Platform Train Incidents are set out in Table 13, 14 and 15.

Table 13: Preventive Risk Reduction Measures – Collision Between Trains

Preventive Risk Reduction Measures	Risk Contributor (Collision Between Trains)
Improve braking systems	***Brake trigger system failure***
Replacement of brake controllers	
Renewal of brake valves	
Additional testing and inspection - to improve test and inspection regimes (specifically brake systems) prior to deployment	
Introduction of alternative / automatic braking systems to improve availability of braking systems	
Introduction of brake failure alarms or detection systems	
EMC studies, monitoring interference levels	***Train Slow or Stopped***
Traction system renewal/refurbishment	

Preventive Risk Reduction Measures	Risk Contributor (Collision Between Trains)
Improvement of processes/procedures (including driver training)	
Further/enhanced/additional operational railway testing prior to operations on live track	
Improve testing and maintenance regime for trainstop, parking brakes for all stabling points	***Train Runs Away***
Enhanced testing and maintenance regime for spring applied parking brakes to eliminate/reduce WSF of the spring applied parking brakes	
Relocation of stabling points - from downslope locations	
SCAT system inspected/tested prior to train leaving the depot - improved SCAT inspection and testing regime	***SCAT Failure***
Modification of train movement procedures and driver training - improved additional training and driver behavioural studies/assessments	***Wrong Direction***
Extensive sighting studies to identify potential sighting problems	
Modification of signalling in line with sighting constraints	
Change to single stopping positions	
Introduction and use of in-cab CCTV eliminating/reducing other person induced constraints on stopping positions	
Introducing train stops in areas where they are currently absent	
Additional supervision to check the aspect prior to the reverse movement	
Track re-alignment to gauge (focus on track stressing & effects of weather) on embankment and structures	***Side Swipe***
Speed restrictions - side swipe	
Driver training - braking techniques	***Service Brake Failure***
Notices on slippery routes	
Alarm/Audible warning of service brake failure prior to brake demand	
Berth track diversity	***Signal WSF***
Speed restriction - Compromised overlaps	***Compromised Overlap***
Overlap studies and potential extension of overlaps	
Enhance braking performance (See 'Improved braking system' above)	
Studies on effect of power in trains (especially for the introduction of new trains) and potentially driver training on specific areas of compromised overlaps (controlling trains - traction power management)	
Train speed restrictions - likely SPAD locations (Signal Sighting)	
Increased overlap in the design of the signalling system - extension of overlaps	***Poor Wheel/Rail Friction***
Introduction of weather forecasting/predictive systems such as ACAT	
Water jetting and sandite	
Procedures (also covering changes to operational concept) and subsequent driver and relevant railway driver training	
Tripcock positions to be re-examined and potential relocation/re-	***Driver Passed Signal at Danger (SPAD)***

Preventive Risk Reduction Measures	Risk Contributor (Collision Between Trains)
installation	
Extend operational testing prior to service for tripcocks, arrestors and SPAD control systems	
Driver training - additional procedures to support drivers (SPAD)	
ATC system introduction	
New/enhanced interlocking system - route locking system	
Introduction of automatic signalling systems - minimisation of human error	
TPWS Train Protection and Warning System	
Modify signalling to align with sighting constraints	
Additional testing and inspection of wheels and rail (NDT)	
Extend overlaps	***Emergency Brakes fail to function***
Additional testing of brakes to determine if brakes are isolated	
Introduction of enhanced braking system - eliminate scenarios where emergency brake signals fail to transmit to brakes (same as 'improved braking')	
Training for maintenance and test teams	
Additional operational testing and inclusion in regime for rigorous asset acceptance/approval	
Rewiring/refurbishment of existing communications/radio systems	***Delayed communications due to train radio system***
Better communication between train drivers and line controllers - communications procedure/driver and line controller training	
Update communication procedure and related procedures for drivers and line controllers	
Modify the train traction system e.g. filters, ICMU (interference Current Monitoring Unit)	***Traction power or track circuit of adjacent line not indication occupied or showing shorted by derailed train***
Extended overlap	***Wrong direction train movement due to signal operator, driver error***
Additional procedures and subsequently, Driver and Signal Operator training - observation that wrong route is set prior to proceeding past signal	***Collision with another train subsequent to a collision***
Points machine failure - new/enhanced point machines with 'route holding diversity'	

Table 14: Preventive Risk Reduction Measures – Platform Train Incidents

Preventive Risk Reduction Measures	Risk Contributor (Platform Train Incidents – Platform only)
Station Master/personnel training	***Crowded platform inhibiting driver's view (crowding)***
Increased train frequency - more trains to cater for peak times/special events such as football matches	
Painted line warnings/signage	
Improve platform lighting	

Preventive Risk Reduction Measures	Risk Contributor (Platform Train Incidents – Platform only)
Built-in access and egress from incident site	
Replacement of door dampeners (design options)	***Door dampener fault – door closing with excessive force***
Replacement of entire train door units	
Improve inspection, testing and maintenance regimes for doors prior to train release	
Redesign/rebuild platform (per platform)	***Passenger falls from platform***
Improve surfaces on platforms and footbridges	
Introduce/improve reporting arrangements of station defects	
Gap fillers	
Crowd control – emergency and incident plans, barrier control	
Platform barriers	
Introduction of new trains to reduce overcrowding (See also more trains to cater for increased traffic above)	***Passenger falls between cars***
Introduction of new trains with open walkthrough between cars - no doors between cars	
Additional platform warnings/signage	***Person pushed from platform***
Platform Edge Doors (half length)	***Passenger strikes/falls against train***
Platform Edge Doors (full length)	
Ventilation system in summer (subsurface)	
Additional station area lighting	
Stair-nose markings	
Speed restrictions	***Trespass on track in station area***
Fencing	
Provision of staff at some locations, specifically to watch for people loitering on platforms	
Closure of access to unused platforms or platform areas	

Table 15: Preventive Risk Reduction Measures – Derailment

Preventive Risk Reduction Measures	Risk Contributor (Derailment)
Inspection and maintenance of suspension to prevent incorrectly gauged suspensions in the depot prior to train deployment	***Suspension failure (per train)***
Improve inspection, testing and maintenance regime for detection of wheel flat and worn wheel failures	***Defective Wheel***
Additional training for route setting personnel	
Speed restrictions	***Excessive speed***

Preventive Risk Reduction Measures	Risk Contributor (Derailment)
Optimising cab design for driver protection in a collision	
Traction/power assessment - introduction of systems such as surge arrestors, current limiters etc.	
Master controller installed in driver's cab for the driver to reduce or apply power to train	
Review of operational concept/procedures for 'proceed under rule'	***Proceed under rule***
Inspection and maintenance of shoe-gear prior to deployment	
Review programme for structural assessments/surveys - potentially more surveys/assessments introduced to existing programme	***Train falls down an embankment or bridge after a fast derailment***
Programme for assessment and management of workload for train drivers, line controllers, signallers and safety-critical staff	
Improve inspection and testing of fish-plated joints - track	
Replacement of fish-plated joints	
EMC studies on trains compatibility with track/signals - monitor interference levels, identification and introduction of relevant immunisation/earthing solutions and potentially further operational railway testing	***Tripcock fails to activate brakes***
Introduce training and competence management schemes for train crew	
Un-obstructive monitoring of drivers and train despatch and subsequent modifications/amendments to despatch rules. Rules for train despatch reviewed/simplified; (procedural change and subsequently, driver training on new despatch rules)	
Improved management processes for train recovery	
Introduction of sequential systems of various kinds such as axle counters and other position detector systems etc, (in addition to track circuits to provide redundancy & diversity)	***Loss of train detection – Train fails to shunt track circuit***
Replacement of track circuits	
Enhanced maintenance/testing such as detailed observation of the track circuit operation and readjustment of the track circuit (operating voltages)	
Review and improvement of recruitment and selection processes	
Examining supervision and monitoring guidelines for operational safety staff, including shunters	
Track re-alignment to gauge (focus on track stressing & effects)	***Track buckling and Side Swipe***
Track inspections - track vehicles	
Track inspections - track workers	
Track refurbishment/renewals (including sleeper management programme to reduce gauge spread)	

Preventive Risk Reduction Measures	Risk Contributor (Derailment)
Track and conductor rail alignment	***Shoe caught under the conductor rail***

5.5 Costs Associated with Implementing the Separate Preventive Risk Reduction Methods

The magnitude of removed risk is a significant part of the selection criteria but the cost considerations are another key element. Costs generally correlate with the magnitude of removed risk achieved. The cost factor influencing the measure's selection is typically a consideration of all measures, including potential alternatives. In some cost effectiveness studies, these are also based on performance factors such as the accident effect on timetables and delays in introducing a new technology. It follows, then, that the risk reduction attained from applying individual measures to specific applications is evaluated by assessing the accident costs and the cost of implementation.

The worksheet for Collision Between Trains presented in the Appendix uses data from previous internal railway economics and safety studies. As far as practicable, the data sets contain information that can support the risk reduction measures selection study. However, this work is primarily for demonstrations of how effectively the risk reducing measures can be used when faced with several choices of varying risk reduction capabilities.

In practice, all factors influencing the operation of a safe railway must be considered. Where this is not possible, a reasonable and balanced method for assessing effects of implementing the risk reduction measure is taken into account. Cost effectiveness studies (discussed in previous chapters) that are undertaken on the railways use similar information to the data provided in assessments of the net cost to operations and performance of the railways. The costs considered include:

- Capital cost and installation cost;
- Changes in on-going operating costs, e.g., maintenance or staff costs;
- Operational benefits - revenue from increased usage as a result of passenger benefits;
- Societal benefit associated with reduction in accidents;
- Potential costs associated with misuse of the safety systems such as passenger error with emergency plungers leading to delays.

The conventional methods of representing the benefits from implementing any of the risk reduction measures is quantified and presented in monetary (cost) units. This representation follows with the simplified rationalisation of the risk reduction effort as the evaluation of the likelihood (probability) of avoiding or averting an accident.

The accurate assessment of the effectiveness of each preventive risk reduction measure under consideration is based on a thorough review of databases and internal company literature on safety studies and subsequent cost-benefit analysis. The under-reporting of accidents or incidents generates loss of accuracy in prioritising railway accidents for subsequent estimations of the economic benefits from risk reduction. A fundamental requirement for assessing accident costs and benefits of a large number of risk reduction measures is to ensure that all measures are compared on equal premises.

In order to reduce the effect of underestimation or non-reporting, equivalent fatalities are built into accident analysis. This has been comprehensively presented in Chapter 2. Incidents on railways are categorised as

- Fatality is considered 100% equivalent fatality
- Major injury is considered 10% equivalent fatality
- Minor injury is considered 1% equivalent fatality

The data set only provides information on actual accident risks and risk reduction with associated costs of implementing the risk reduction measures, i.e. capital, installation and maintenance costs for the operational time/duration. The key assumptions used for this evaluation include an operational time of 10 years and the incorporating of a discount rate of 5%. The latter is employed to demonstrate the flow of costs and risk reduction. The future values calculated help illustrate in present terms that a cost-effective risk reduction is attained from the introduction of the risk reduction measure.

Accident costs are estimated based on standard unit costs for accidents. The risk reductions achieved by the various measures are then compared to the cost of implementation. The challenge is that the costs of implementing the risk reduction measures are typically expressed in monetary terms. However, the risk reduction (reduced fatalities and injuries) are not conventional ‘traded goods’ and they do not have direct monetary values.

In order to express the accident risk reduction in monetary value for subsequent effectiveness assessment, the reduced risk of particular contributions to an accident, for example, derailment is estimated using the value of preventing a fatality (VPF) for 2010. This is approximated as £1.7 million.

Additionally, it is worth noting that the cost of the risk reduction measures decreases over time, potentially making present and least cost-effective measures cost-effective in the future.

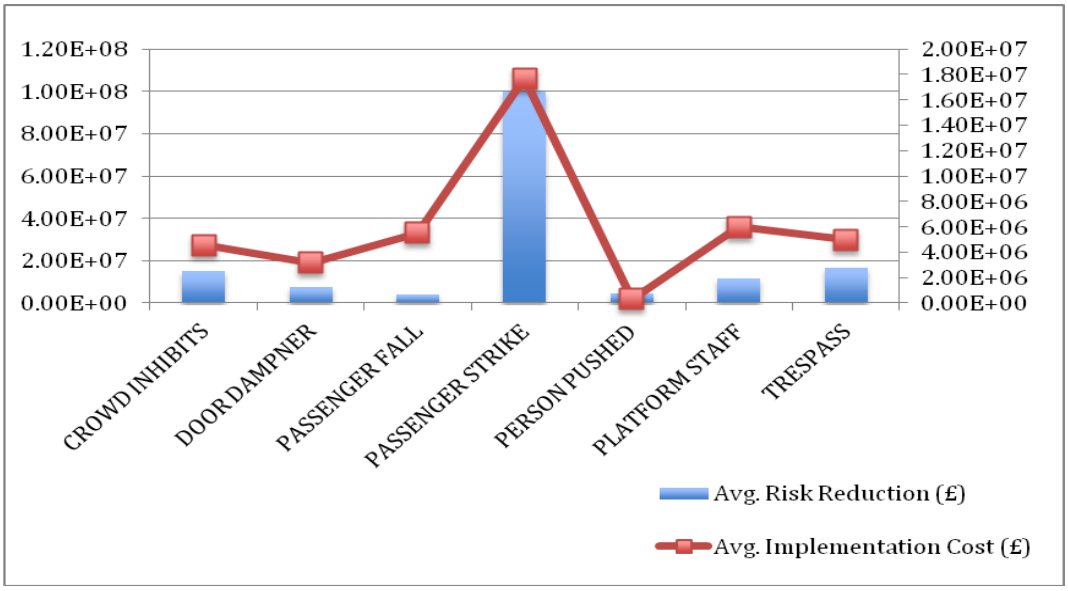


Figure 34: Application of preventive risk reduction measures – PTI

Figure 34 illustrates the extent of current investments in line with the ALARP requirements. However, the 'Passenger Fall' risks and current cost benefit practice, the charts indicate that the cost of implementation exceeds 3 times the benefit. Risk reduction measures such as platform barriers, gap fillers, improving surfaces or redesigning platform with risk reduction considerations are all considerably capital intensive when compared to the risk reduction benefit possible. In evaluating this particular risk, most projects tend to centre the cost effectiveness case on other cheaper but less effective measures by using the ALARP framework to introduce measures such as crowd control, stair-nose markings and additional platform staff.

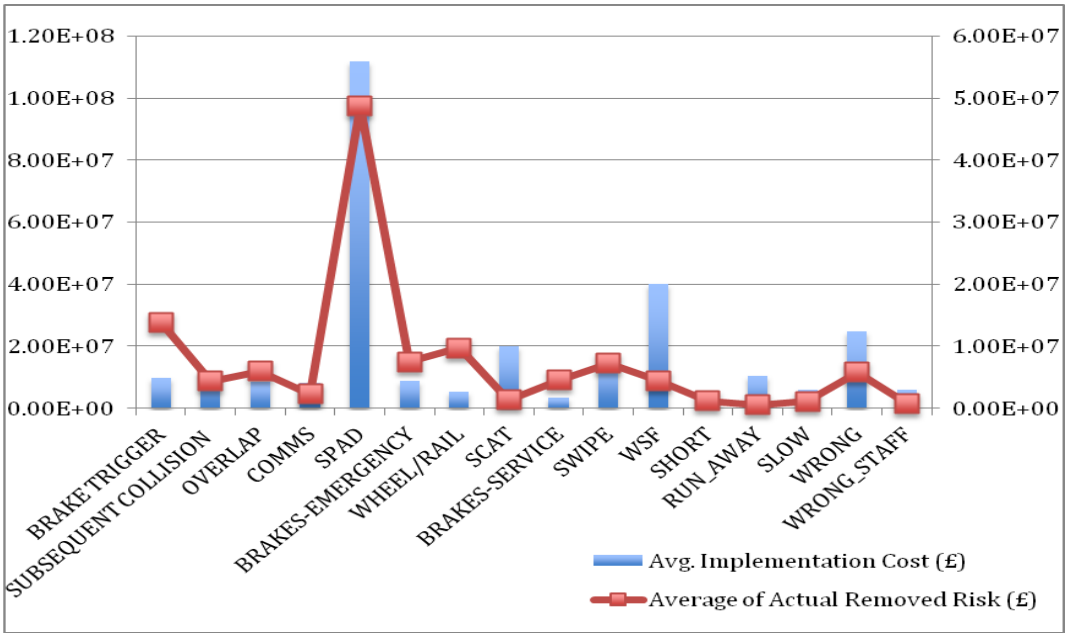


Figure 35: Application of preventive risk reduction measures – Collision Between Trains

Figure 35 presents the disparity between SPADs and low risks such as slow train movement, SCAT failures and runaway trains. All of these risks contribute to Collision Between Train accidents. This chart clearly indicates that the current risk reduction measures for 'brake failure' and 'wheel/rail interface' provide a great amount of risk reduction for their costs. On the other hand, the cost of implementing measures to reduce 'Signal Wrong-side failures (WSF)' is typically over the factor of 3 considered during cost benefit ALARP studies.

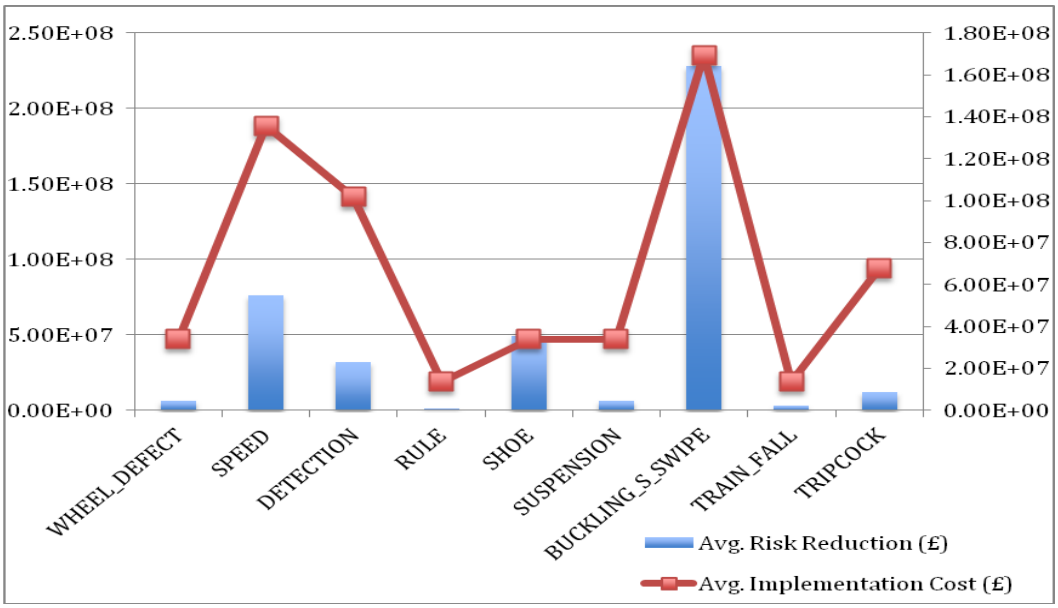


Figure 36: Application of preventive risk reduction measures - Derailment

Slightly different from the previous charts, Figure 36 shows the need for capital-intensive measures to reduce the risks introduced by contributors to the Derailment accident type. The figures demonstrate the need for a structured method for optimising cost and risk reduction measures.

5.6 Constraints and Considerations in Selecting Preventive Risk-reduction Measures

The core principles guiding the selection of preventive risk reducing measures generally ensure that accidents are avoided, that there is reduced impact on failure, reduced vulnerability, and increased resilience.

The current practice of selecting risk reduction measures by simply prioritising based on the estimated (quantified) risk reduction and the imposition of the preventive-first principle is misleading and potentially counter-productive. Without consideration of the consequences in the event of the accident, this further exposes railway operations to major incidents and fatalities or unnecessarily increases the cost of the risk reduction measures by costing expensive measures for accidents with small impact. The

examples presented here also show that two options with similar estimated risk reduction will not only have different costs but will also be suitable for certain applications and not to others.

The constraint of applying measures for particular risks therefore depends on a thorough understanding of the accident; all possible scenarios that could lead to the accident including the contributors to the accident; the impact of the accident and potential measures to reduce the accident to ALARP. This effort demonstrates that the effectiveness of the risk reduction measure selected must be based on a thorough understanding of the primary functionalities (attributes and limitations) of all measures within the application. This in effect means that we have failed to achieve the estimated magnitude of risk reduction by simply selecting the cheapest measure or the one with the highest benefit-cost ratio.

Preventive risk reduction measures are effective in areas where the intervention subsequent to an accident is difficult: restricted access areas such as tunnels/tunnel railways, as is the case with London Underground (with both underground and sub-surface lines), Glasgow underground metro, or the Channel Tunnel Rail Link. In such cases, the selection of a protective risk reduction measures over a preventive measure must incorporate additional factors and associated costs such as:

- Access and egress requirements
- Hand-back of line section
- Training and availability of emergency services for special scenarios such as restricted access
- Track-side safe areas designed and constructed into the railways
- Tunnel telephones, alarms
- Emergency lighting and signs
- Ventilation for tunnels

The risk assessment of the railway must be based on a benchmark railway risk reduction target for the existing infrastructure. In practice, most contractual railway risk reduction requirements clearly state that the introduction of risk reduction measures must at least, maintain the existing risk level of the operational railway. This invariably means that the relevant interfaces associated with a railway will have to be assessed to ensure that the risk level is at least maintained, following implementation of these measures. This implies that the implementation of a preventive risk reduction measure must consider its impact on the specific risk but also on all other systems, interfaces and activities so as not to affect the performance and safety of the railway. This is a major challenge when evaluating and managing railway risks. However, it is important that a holistic methodology is considered.

Selecting effective preventive risk reduction measures is dependent on historical data and an analysis of the improvements required to meet specified targets. However, accurate forecasting of future risk is

often fraught with uncertainty. There may be variations in train lengths, operational rule changes, introduction of new technologies/systems with associated risks, considerations of the number of passengers, number of trains and traffic growth, additional line sections, points, stabling lines/depots, platform or station staff issues, and so on. Such factors influence accident or fatality rates which may invalidate the preventive risk reduction measure(s) subsequently.

As discussed in Section 5.3, such an analysis only focuses on the preventive risk reduction measures that reduce accidents with associated fatalities and injuries (equivalent fatality ratings). Other key components of a conventional economic assessment such as performance related factors are not incorporated. The scope of the work deliberately omits assessment of effects, for example, the distribution of the consequence of an accident on the operational railways following an accident. The extent to which the distribution of accidents is presented is in the assessment of the 'collision after a collision' risk contributor to the Collision Between Train accidents. This in itself is insufficient for a thorough consideration of performance and potential ripple effects such as the consequences of delays leading to overcrowding following an accident.

However, the comprehensive evaluation of risk contributors and risk scenarios is a key requirement in identifying the preventive measures. It is a major challenge in itself. Establishing credible accident scenarios requires a good knowledge of major accident risks on operational railways. Brainstorming sessions on hazard identification sessions with experienced industry personnel are valuable. The illusion of absoluteness can result in a level of uncertainty that can undermine the case for risk reduction. Considering that the 'prevent-first' principle is typically employed, an assessment gradually builds in high levels of uncertainty - a major weakness in the overall risk management process.

Data limitations also affect the accuracy of the evaluation of preventive risk reduction measures. It is therefore important that qualitative means to reduce the impact of the inevitable inaccuracy of data are developed.

Preventive risk reduction measures may not be relevant or effective when acting to address well understood hazards or accident scenarios such as 'crowded platform inhibiting driver's view'. Typical preventive risk reducing measures, such as platform barrier designs, CCTV in the cab and on the platform; extensions to platforms; introduction of longer trains with associated platform modifications; platform edge doors (half or full length), are undeniably expensive and require long-term planning and disruption/delays to put them in place.

In such cases, consideration must be given to a cost effective solution with substantial risk reduction, such as procedural approaches. These approaches with impact-reducing attributes, such as 'emergency

timetables' allow for the increase or decrease in the number of trains in service. Emergency timetables are used to ensure appropriate localisation of any accident on the railways or to relieve the railway from other potential contributory factors to accidents such as overcrowding, system failure, disruptions and delays. Other measures to be considered are additional staff presence on platforms; physical constraints on platform access, in combination with crowd control procedures, and more training in reducing the accident scenario.

As mentioned in previous chapters, e.g. Section 2.5 and subsequent sections, it is obvious that training, monitoring and supervision are essential for the effective implementation of preventive/risk reduction measures. A typical example is the stressing of track against buckling. This can only be effective if training on buckling and stressing is provided for track engineers. Drivers must also be trained on actions to prevent incidents such as identification and reporting of track misalignments. In addition, the monitoring of weather and track movements, and subsequent supervision, developing a structured track maintenance programme, is required to achieve optimum standards

The success of accurate prediction and prevention of major accident risks requires that the root causes of failures be addressed, whether they are organisational weaknesses, poor management systems or culture. At present, the relationship between selection, implementation, and the environment/structure for ensuring that the risk reduction measure is adequately applied is rarely considered. It is however a standard requirement for developing a safety case: this is a demonstration that the risk reduction measures are efficiently managed through the life of the project or system. However, analyses of preventive risk reduction methods employed are typically relegated only to basic cost effectiveness studies.

The current practice of risk reduction selection fails to account for how one measure affects others - an essential factor for the decision-maker. These and other constraints illustrate that assessing preventive risk reduction measures alone derails the effort for accident reduction. The identification and subsequent selection of risk reduction measures must be supplemented by additional information on the functionalities or capabilities of all other possible measures, before embarking on a comprehensive and structured selection process.

Preventive risk reduction measures, conventionally used as a priority to eliminate or reduce the likelihood of an accident, may result in additional risks that have to be balanced by additional measures whether preventive or protective. The risk reduction achieved by measures proposed for reducing particular risks or accident scenarios must be tempered with the realities of their application. For example, dry sand as a preventive risk reduction measure can be effectively used to improve rail/wheel

friction but the application must be controlled to ensure that the sand does not build up an insulating layer on the rail/wheel surface. This likelihood should be factored into the estimated risk reduction. The use of axle counters which is also a preventive risk reduction measure as a replacement for track circuits has its limitations. It is misleading to claim 100% effectiveness as the axle counter cannot reliably detect all wheel sizes from some trains.

Chapter 6 Protective Principles and Techniques for Reducing the Risk in the Railway Industry

As a result of technological advances such as improved signalling systems, train control systems etc., together with system user training/awareness and other efforts towards preventing the risks of accidents (Chapter 5), major railway accidents are becoming less frequent. However, the potential for incidents and major accidents - still exists. This was demonstrated in recent accidents in China and Spain where several lives were lost both at the site and subsequent to the event. Protective risk reduction measures are applied to reduce the consequences or cost of an event/accident.

The correct choice of protective measures ensures that fewer fatalities and injuries are realised: for example, the introduction of crash-worthy vehicles significantly reduces the risk to passengers in events such as impact, falls from trains (non-sensitive, slam doors on moving trains), passengers getting caught between train doors, the opening of wrong side doors, etc. Various protective measures are considered in this chapter, in order to provide a comprehensive assessment and structured thought on the application of protective risk reduction measures on the railways.

In line with the overall objective of maximising risk reduction within a fixed budget, this chapter offers an essential understanding of the characteristics of protective risk reduction measures by using the basic principles of risk reduction through reducing the consequences from risks which materialised. This understanding will provide the clarity required within the industry on measures for reducing the consequences of an accident, and their relationship with other measures for cost-effective risk reduction. The foundation for selecting protective measures that comprehensively support the case for maximum risk reduction is developed in the following subsections.

6.1 Protective Risk Reduction Requirements, Principles and Systems

Railway risk reduction requirements identified in most railway operational safety cases are presented in Section 5.2.1. It is worth noting that a thorough evaluation of these safety cases showed a heavy reliance on preventive risk reduction measures demonstrating that minimal effort is put towards assessing the impact of protective measures on risks. As stated in the introduction to this chapter, accidents cannot be totally prevented as risks exist and undoubtedly propagate quickly if controls are not incorporated in system design and operations. Furthermore, protective measures are necessary for the simple reason that not all possible risks can be identified. In this case, the only barrier reducing serious consequences is the protective barrier.

Effective protective measures for risk reduction contribute to achieving the control of major accident hazards. They are reactive measures and do not prevent accidents from occurring. However, if applied

correctly, they can significantly reduce the consequences of an accident by limiting their development, magnitude and duration.

In the absence of well-defined and fixed primary protective requirements on the railways, this section summarises the case that systems with protective features must be designed, manufactured, constructed and maintained. It is argued that as far as is reasonably practicable, they should minimise the risks of escalation following an accident under normal and abnormal operating conditions or when such operations are subjected to malicious acts.

6.2 Application of Protective Risk Reduction Principles

The basic risk reduction principles, i.e., relationship to fundamental railway risk reduction (safety) requirements and associated applications in the railways, are presented here. Figure 37 provides a simple illustration of 12 key protective risk reduction principles (Weli and Todinov, 2013a).

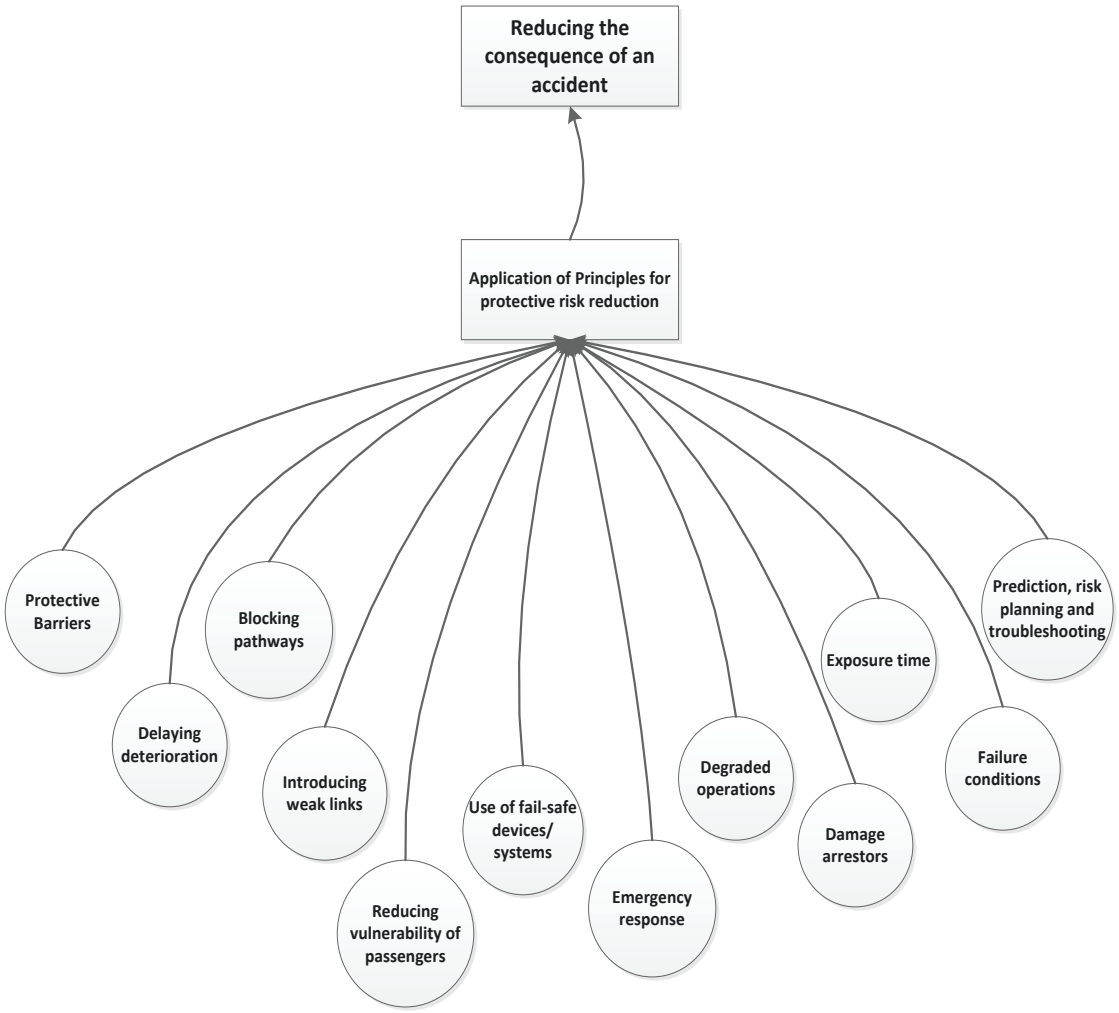


Figure 37: Protective Risk Reduction Principles

6.2.1 Protective Barriers

The use of such barriers on the railways has typically been classified as physical or non-physical for prevention or mitigation, protection or management, of undesired accidents. This basic understanding helps to provide a platform for developing protective barriers. However, a more detailed analysis would be required for the appropriate application of safety barriers in specific cases, such as collision, derailment and platform train incidents where protection plays a significant role after such an event.

In the process industry, where protection also plays an extensive role in risk reduction, studies have been undertaken to reduce the ambiguity of protective barriers and their applications. Sklet (2006) attempts to develop common terminology, classification and attributes to enhance the understanding of the concept and performance of safety barriers. The study narrows down so-called safety barriers to a description of their condition, functionality, reliability, response time and robustness.

Todinov (2007) uses the release of a toxic substance to demonstrate that the effectiveness of protective barrier measures is dependent on a combination of a number of barriers, i.e., passive physical, active physical, immaterial, individual/ organised human action, and recovery barriers. Harms-Ringdahl (2009) also provides a method for identifying improvements due to the application of safety barriers by proposing the integration of technical, organisational and human functions.

The combination of the studies for classifying and applying protective barriers in line with the objective of this work considers that for a protective barrier to be effective, the following must be fundamental requirements:

- Comprehensive understanding of specific risks and their impacts
- Function and scope of the barrier – what can practically be achieved with the protective barrier
- Operational constraints
- Complementary measures - additional systems, processes etc., to meet risk reduction objectives

6.2.1.1 Passive Protection Barriers

Implementation of passive protective barriers on the railways requires the use of separation mechanisms, techniques, or materials to isolate the accident from the target. A good example of a passive protective feature is the use of thermal barriers such as passive fire protection systems to reduce the risk of fire escalation.

The introduction of thermal barriers for tunnel railways such as London Underground was in response to major accidents such as the King's Cross Station fire. This technology, transferred from the petrochemical sector, is spray-applied or designed into concrete and steel structures as effective resistance to heat. This

risk reduction measure ensures that in the event of a fire, the safety of passengers is improved by extending the period of full operations. In order to achieve this, the integrity of the tunnel structure has to be maintained until the passengers are delivered to safety. .

Stabling track areas are effective means of isolating trains and passengers from escalating accidents on a network. Following an accident on a line, the risk of a follow-on accident or exposure to an already escalating accident can be significantly reduced.

Visual and tactile warnings such as safety zones or stair-nose markings are commonly used along platform edges, depending on the speed of a train for the particular platform or line section, and/or giving protection against the aerodynamic force of a train or slipstream effect of a passing train. Similarly, passenger information systems provide regular updates on the state of operations within the platform and, on the railways, provide the passenger with information on actions following an accident. This intangible risk reduction measure will not fall into the standard categorisation of physical barriers, as in current standard classification.

The effectiveness of these protective barriers depends significantly on human contribution, as in effective platform supervision.

6.2.1.2 Active Protection Barriers

Active protective barriers are mechanisms for reducing the consequences of failure by triggering (manual or automatic) protective systems.

The operation of emergency braking in conventional signalling systems is a good example of an active protective barrier system. Trainstops operate a tripcock in a raised position to trigger the brake valve and activate Emergency Braking (EB). This is an example of an active protective barrier against further incidents following a SPAD.

In the event of an accident on the railway, risk reduction can be achieved by de-energising traction power for the affected areas to permit the safe detrainment of passengers. This is a fundamental feature in any railway system: the active de-energising of power is paramount in the event of an incident or accident, and an absolute requirement for tunnel railways.

After a derailment or collision, the activation of Correct Side Door Enable (CSDE) systems provides a means of restricting the passenger to the safe doors.

6.2.2 Damage Arrestors

Automatic de-energising or isolation to trip systems can successfully reduce the escalation of a failure, e.g. over-voltage protection systems. The effect of incidents such as pantograph arcing, induced switching surges from AC systems, short circuits, insulation flashovers, trespass and damage can be further reduced if the application of the 'damage arrestor' principle is employed by the use of over-voltage protection and isolation measures.

Derailments have been known to result from the shunting of adjacent tracks, thereby energising the train and track. Isolation and de-energisation techniques and systems ensure that the affected derailment or collision sections and their adjacent sections are automatically de-energised, to eliminate the risk of electrocution.

Other measures with this application for risk reduction in the railway industry include flame arresters, and stations and central control facilities designed for structural integrity, with growing requirements for explosion and fire containment features.

6.2.3 Blocking Pathways through which Accidents Escalate

After an accident such as a derailment or collision, a secondary accident can potentially increase the severity of the first. The potential for a second accident scenario on the railways means that the passenger is exposed to additional safety risks. For passengers remaining on the initial accident train, the increased risks are:

- Train hit by a second train
- Fire escalation
- Collapse of structures

For passengers evacuating the accident train, the compounding risks are:

- Crushing or stampede as a result of evacuation chaos
- Electrocution of passengers by conductor or power rails (traction power)
- Passengers struck by passing train

The principle of blocking routes for accident escalation (i.e. accident after an accident) is an efficient method of limiting such consequences. This can be achieved by various applications, and/or various individual/combination of risk reducing measures, to attain the operational safety targets.

Most emergency stopping or braking systems used on the railways, when activated, prevent further propagation of an accident or the effect of an accident. Examples include the operation of Emergency

Braking (EB) through activation of Tripcocks and the use of Platform Emergency Stop Plungers (PESP) on platforms in order to stop a train approaching a platform. Other frequently used risk reduction measures with similar attributes to block pathways to accident escalation are: crowd control; automatic signalling systems with automatic inhibit functions for reducing human errors during an accident; route locking systems; buffer stops; fencing or restrictions to the access to an incident; platform edge doors (half and full length); closure of unused platforms or platforms areas; gap fillers; improved door control mechanisms such as selective door operations; emergency lighting, clear paths or signs to emergency exits within trains in the event of an accident; and lastly the de-energising of power for the route or line section.

System operational features on trains such as selective door operation, or correct-side door enable, are risk reduction measures normally used as preventive risk reduction measures at short-length platforms. However, the systems also have enhanced protective features for blocking paths to the escalation of an accident.

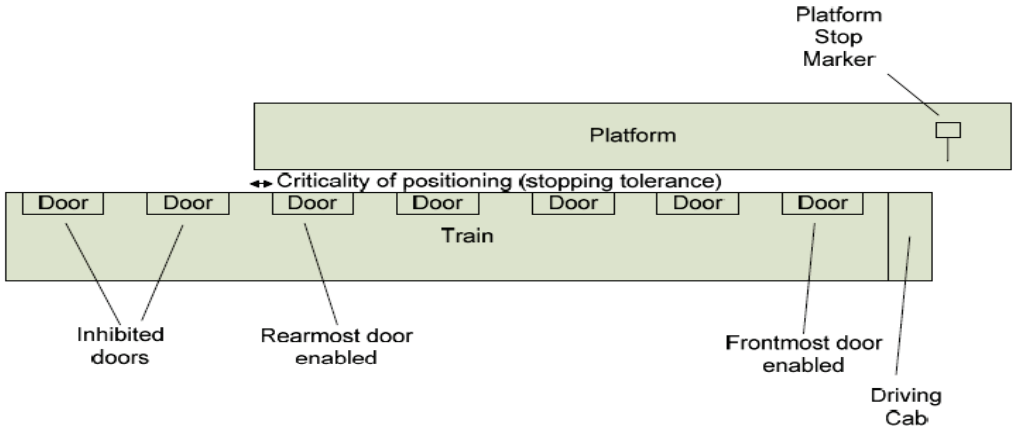


Figure 38: Platform Train Interface – Door selection for risk reduction

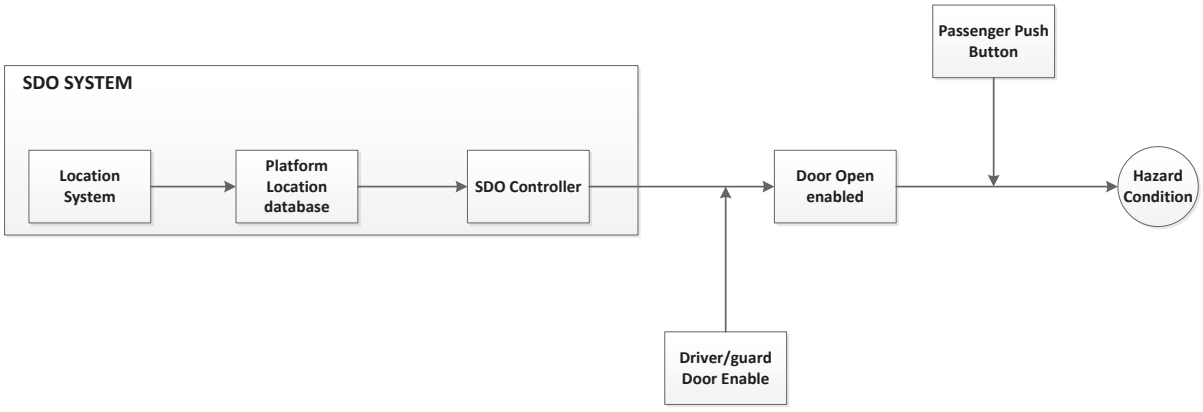


Figure 39: Selective Door Operation (SDO) system for Risk Reduction

The selective door operation feature on trains involves the opening of some doors and the inhibition of other selected doors, either manually or automatically. On newer trains, this application usually operates. Further, the automatic train door selection system determines specific doors to open at a given station (see Figure 39 above). The automatic train selection system also provides audio and visual information of the doors closed. This information helps direct passengers to leave the train through the appropriate sections or doors. The correct side door enable and automatic train door selection acts as a means of blocking further risks of accidents in scenarios where detrainment of passengers is required, following a failure or accident. Such scenarios may include trains that are stuck in a tunnel, or in areas where there is the risk of electrocution from alighting due to the presence of a third rail, or adjacent running lines with the risk of trains passing.

6.2.4 Using Fail-safe Devices

Fail-safe systems have already been comprehensively addressed in their use as a preventive risk reduction measure; however, the fail-safe principle is also used as a protective measure. It is worth noting that there are several railway applications of fail-safe systems for protective measures that are effective and must be considered in studies of risk reduction and cost effectiveness.

The use of isolation techniques such as emergency power cut-off switches or stick relays to de-energise track circuitry following an accident is an effective protective risk reduction measure.

The driver uses the driver's brake valve to control the brake release, running, lap, application, emergency and shutdown positions for operating and locking the valve out of use. The use of the brake valves in emergency scenarios for reducing the consequences of an accident is essentially a protective risk reduction measure.

Brake valves are predominantly susceptible to random and design-related failures. The failures and their impact are minimised by employing fault-tolerant, fail-safe techniques in brake valve systems designs. Supplementary measures include introducing and adhering to quality management practices during the design and implementation lifecycle.

The implementation of 'renewal of brake valves' as a measure for reducing the impact of an accident such as Collision Between Trains is primarily a design feature that allows for both the reduction of the likelihood of an accident and minimises the cost of such an accident.

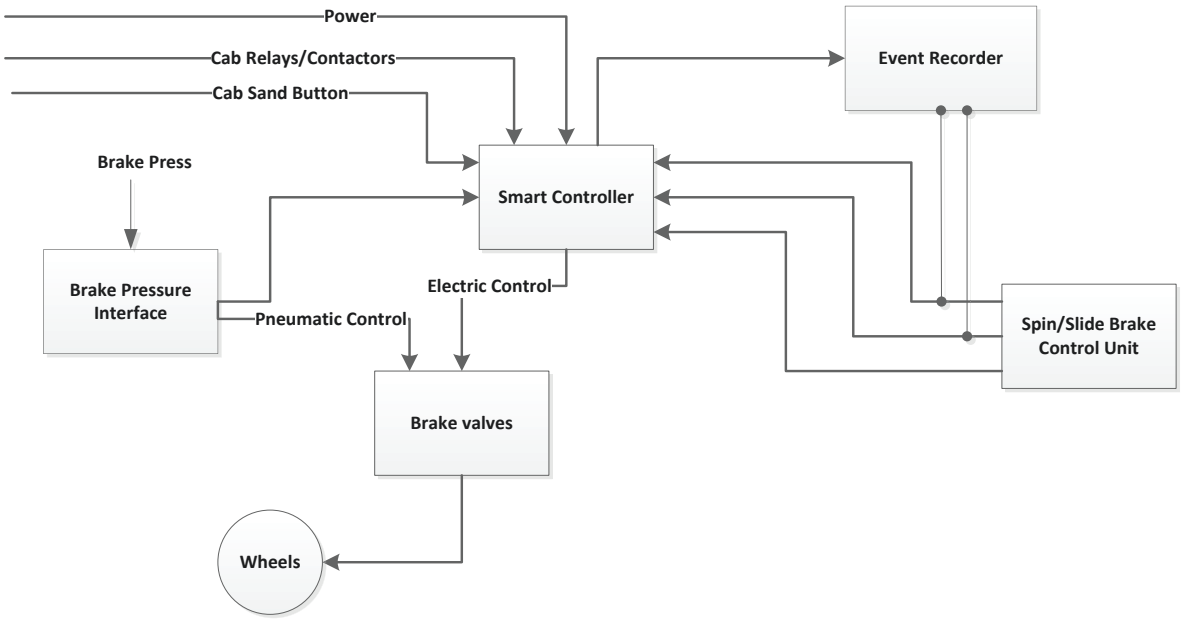


Figure 40: Simple block diagram of an Electro-pneumatic braking system

6.2.5 Introducing weak links

There is a growing need to understand accident survivability with regard to structural 'crashworthiness' and the dynamic stability of trains in the event of collisions. This requirement is fundamental to cost-effective risk reduction for the R&D of train operators and manufacturers.

RSSB (2006) presents studies using past accidents statistics to demonstrate that casualties are significantly reduced when vehicle stability is maintained following a collision or derailment, and that there is consequently a benefit in furthering the understanding of collision dynamics and stability. The study concludes that despite the consensus in the industry that incorporating crashworthiness features into new-built trains is cost-neutral; there are risks and costs involved with the design and development of such features.

The most stringent train car design standards simply require that these designs address the reaction of under-frame proof loading, and mid-collision post-height, without clear requirements on energy absorption or other dynamic loading requirements. The Crash Energy Management (CEM) design incorporates several sacrificial crush zones with progressively increasing force-crush characteristics. This design came out of the need to develop a vehicle end crush zone that would improve the energy absorption capacity of the train structure. In order to prevent the front train cars from absorbing all the energy from a collision, crush zones are introduced to allow the distribution of energy between trains and train cars. This distribution of collision energy is a vital protective risk reduction feature as it helps to

ensure that the trains remain on-track, rather than go into vertical displacements in the form of jack-knife buckling and subsequently derailment.

In the event of an accident, the design of emergency exits in order to reduce the severity of injuries is a major decision for railway operators and train systems suppliers. Some train cars are designed to enable the use of the sidelights for identifying emergency exits. However, the overall risk reduction case includes breaking of the glass with a hammer, specially designed for escaping from an accident. The glass must be the toughened float glass type to enable easy exit. The use of toughened glass in this application is a protective risk reduction measure. However; the specific application of introducing a weak material into the design has its disadvantages, as there may be a greater need to keep the passenger from being expelled from the train during a collision or derailment. Toughened glass in recent railway train designs is also limited in its ability to prevent the impact from external objects flying into the train during an accident.

6.2.6 Delaying Deterioration

The application of fireproofing and insulation coatings on materials used for structures in tunnels and railways in general is only one way of delaying deterioration in the event of a major accident such as a station fire. The principle of delaying deterioration is of significant importance and effective in risk reduction applications if additional measures such as emergency/incident plans, adequate station layout designs (egress or emergency exit), crowd control, clear and unambiguous signage, instructions and guidance from station supervisors or station staff etc. are used to supplement it. If it takes a calculated time interval to exhaust the protective power of fireproofing and insulation, it is necessary that in this window, measures are available to remove the target from the hazardous area.

A practical railway challenge for train drivers, however seldom it occurs, is running with isolated emergency brakes. To reduce this risk, designing robust emergency brakes is only a part of it. In combination with precautions, procedural modifications and subsequently, the training of drivers is essential to achieve the risk reduction.

Speed restrictions subsequent to an accident could potentially delay deterioration, if action is taken in the very short period following the accident. Other similar applications of this principle include structural reinforcements, safety design considerations using technologies on crash worthiness and the strengthening of vehicle interiors (i.e. the CEM project).

6.2.7 Reducing Exposure Time/Duration

The impact from accidents can be significantly reduced by the inclusive design of stations and platforms (i.e., the safety in design philosophy). Basic items for egress and access such as steps, stairs, ramps and

doors can be designed to take into account the reduction of time of exposure to a hazardous situation, if one arises. An example of such a situation is the Kings Cross (London) Underground fire in 1987. HSE (1996) presents a comprehensive report on the upward flame spread on inclined surfaces with considerable channelled power, demonstrating the 'trench effect'. This is a well-known and established fire propagation mechanism, used to describe and illustrate these events on enclosed slopes such as escalators or stairwells in building structures.

With a good knowledge of risk contributors such as trench effect, stations and platforms designs, the materials (e.g. fireproofing) used and physical layouts (escape routes/emergency exits and egress) can be better designed, to ensure the best opportunities for people to survive major accidents such as fire in railway tunnels.

Another practical yet effective example of reducing exposure following an incident or accident is 'signage and way-finding at stations'. Clear and consistent signs, instructions or ways to find exits facilitates easy egress thereby reducing exposure to any consequential effect of an accident. This applies to platforms or trains.

6.2.8 Reducing Vulnerability of Passengers

The use of closed circuit television (CCTV) is an essential measure for reducing the vulnerability of passengers to hazardous circumstances. The train driver will not start the train once he is aware that passengers are stuck at the door, fallen onto the track, or fallen between train and platform. This in effect substantially reduces the severity of injuries that could potentially be sustained by the passenger. An alternative to the CCTV in risk reduction measures analysis is the Platform Edge Doors, which principally reduces platform-related accidents by significantly reducing the direct passenger-train interface resulting in the minimisation of accidents frequency.

Other effective measures for reducing the vulnerability of passengers include platform supervision, crowd control and enhanced door systems. The enhanced door system consists of:

- Sensitive Door Rubber Edge
- Automatic Door Reversing
- Door Emergency Unlocking
- Door Closing Signal

These measures, in combination with in-cab CCTV (for the driver to monitor passenger movements around the platform-train interfaces) achieve a net positive effect on the risk reduction objective.

Ready to depart (RTD) indicators or repeater signals are different ways of informing the platform staff that the driver has permission to depart the platform and also reduces the vulnerability of passengers. Platform area safety systems that can effectively reduce vulnerability when an individual or a combined application for the risk reduction is required include:

- CCTV station and track
- CCTV platform
- Station track supervision
- Intrusion detection
- Coupler area supervision
- Platform boundary door supervision
- Emergency stop plunger
- Fire detection, alarming and suppression systems
- Emergency lighting

6.2.9 Emergency response system or operations

The emergency preparedness concept in relation to this principle and its application as a protective measure on the railways aims to assist in preparations for and responses to occurrences of incidents or accidents in a timely and effective manner. A typical example of an emergency response system is the 'emergency timetable'. This is used as a contingency plan for dealing with severe disruption. Communication and feedback of information to and from line controllers, train drivers and other front line personnel are fundamental to the effective application of this principle. The factors essential to the effectiveness of emergency preparedness, depend largely on training. The need for training to facilitate emergency response planning is highlighted in all the railway emergency preparedness strategies that have been studied as part of this project

Production of emergency timetables usually requires a dedicated team of trained experts in this area. The dissemination of timetable information to all personnel, especially operational personnel, following an accident is usually undertaken by communications experts. Other systems and operations with the application of this principle for risk reduction include:

- Provision of hammers at strategic locations within those train cars for emergency exit
- Introduction or implementation of crowd control procedures or processes (i.e. station and platform area crowd control)
- Increased traffic - more trains to cater for peak times/special events such as football matches, i.e. the introduction of new trains to reduce overcrowding

6.2.10 Degraded operations

A degraded mode of operation is normally characteristic of a train not operating under normal signals or signalling arrangements. This is more difficult to achieve with new train technology such as communication-based train control systems as compared to conventional signalling systems. Typical causes or conditions resulting in degraded operations include signal equipment failures, failure of block signalling equipment such as joints, signal passed at danger, movements during possessions, level crossing failure or track circuit failure.

Accidents do occur during degraded railway operations however degraded operations can also be the only means of reducing the impact following an accident. In advocating this principle for use in application for effective risk reduction, care must be taken to ensure that concepts such as the 'integrity envelope', introduced by offshore operators, are considered. Integrity envelopes ensure that alternative systems and work-around procedures are identified by using operational hazard assessment techniques. The derived potential failure scenarios are then known upfront so railway operations personnel know what the options are and what decisions to take and how long to operate in that state in the event of an accident and subsequent degraded operations.

The railway rule books provide guidance on what actions to take in response to an accident via degraded working. If the accidents or incidents that result in degraded operations are infrequent, there is a greater risk of the unfamiliarity of staff with the appropriate actions. This potentially leads to incorrect responses or mistakes.

Emergency timetables, operating rules (manual, protected manual and fully automated), speed restrictions, training of front-line personnel such as controllers, platform or station supervisors, train drivers, failure reporting, maintenance and testing, part service suspensions etc., are all essential to successful application of degraded operations and the transition from degraded to normal operations.

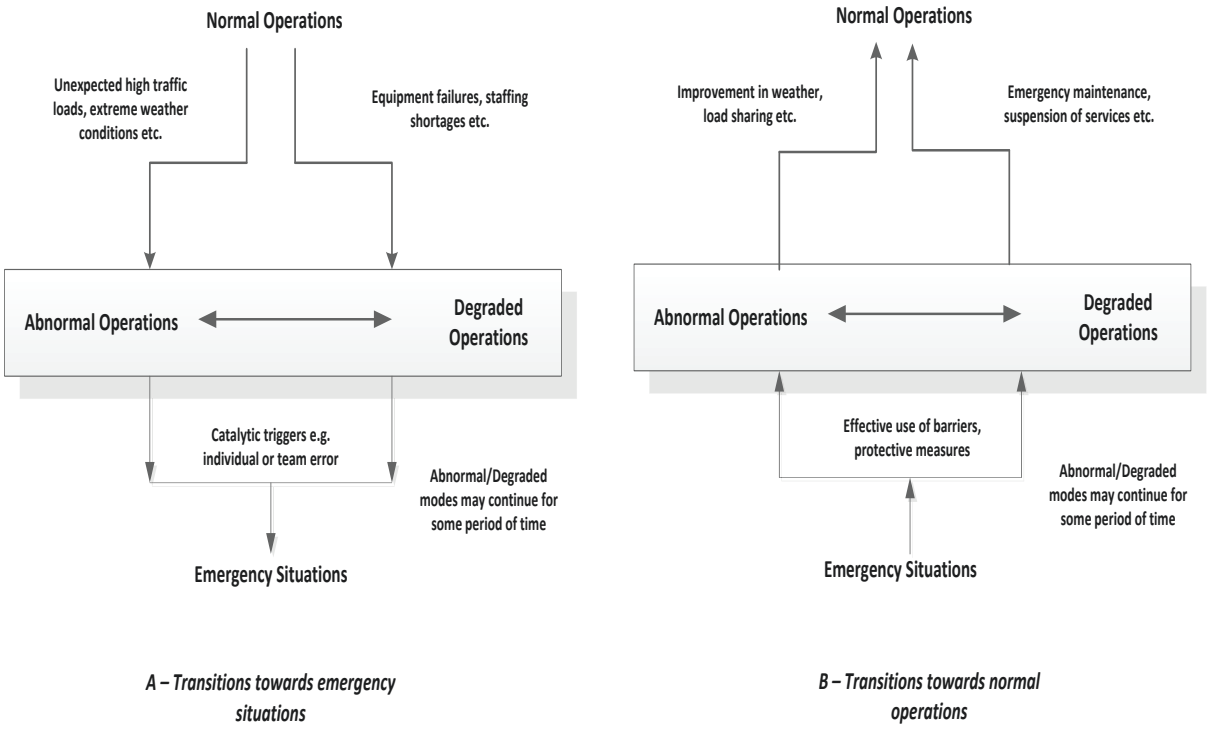


Figure 41: Degraded operations and transitions (adapted from http://www.dcs.gla.ac.uk/~johnson/papers/degraded_modes/Johnson_Shea_Rail_Submission.pdf. Accessed 24-07-13.

6.2.11 Failure indication

With the move towards controlled train operations that provide a comprehensive suite of safety applications, railway systems designs have to provide feedback on system failures, including the actions of operators. The diagnostics and feedback features are now considered a standard safety requirement and are captured in most operational safety requirements justifications.

The AWS is a fail-safe device primarily introduced into railway safety operations as a means of protecting against large accidents subsequent to incidents, such as SPAD. Failure indicators such as the Automatic Warning System (AWS) are only effective for risk reduction if the train driver acknowledges the warning and acts to make the operations safe by braking or applying similar measures.

The AWS alerts the train driver through an audible indication about the aspect of the next signal. The driver is then required to acknowledge by cancelling the horn and potential automatic brake application. The system includes a relay control unit, electro-pneumatic valves connected to the braking system, an indicator in the train driver's cab, driver's AWS acknowledgement button, a control panel (including re-set plunger), a magnetically activated receiver under the train, operating voltages provided by a static

voltage converter, and an isolating handle. A study of the effectiveness of the AWS and the eventual need to discontinue its use is provided in HSE (2001).

Train Protection and Warning Systems (TPWS) are widely used to replace or supplement the functions of the AWS. However, it is still limited in its application as a high integrity train protection system. Internal railway studies have shown that it provides a 60% to 70% reduction in equivalent fatalities caused by SPADs. Failure status monitoring and reporting as part of overall safety and performance is a standard functional requirement of automatic train protection. The TPWS does not have full Automatic Train Protection system functionalities such as failure status monitoring and reporting. Similar failure indications used to good effect to warn of incidents that might escalate into greater degree of loss include Passenger Emergency Alarms, passenger/customer information systems, and fire detection systems (high integrity systems for tunnel railways). However, these are more effective with crowd management processes.

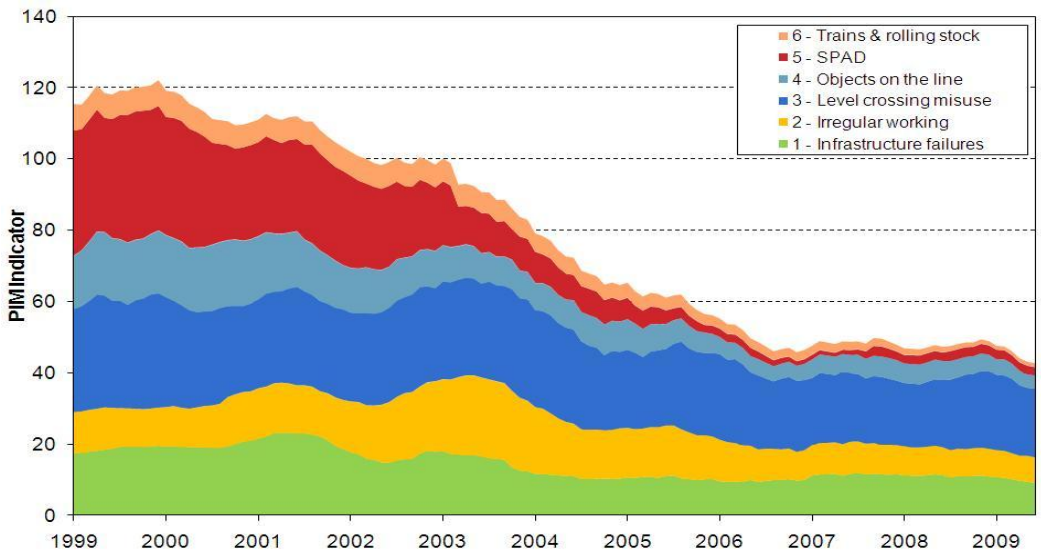


Figure 42: Effective use of TPWS for reducing train accidents (adapted from RSSB TPWS strategy)

Railway systems that rely on the failure indication feature, despite the built-in reliability or fault tolerance, still have the weakness of 'the failure to correctly indicate'. This requires its own study, considering the effect on accidents if incorrect feedbacks are provided during train operations. Leveson (2004) acknowledges that the accurate collection and analysis of data by computer systems to determine whether the system is moving toward the boundaries of safety is difficult and complex. The paper suggests using system accident models and the basic concept of safety constraints to provide directions for:

1. Identifying appropriate safety metrics;
2. Determining whether controls over these constraints are adequate;

3. Evaluating the assumptions about the technical failures and potential design errors, organisational structure, and human behaviour underlying the hazard analysis;
4. Detecting errors in the operational and environmental assumptions underlying the design;
5. Identifying any maladaptive changes over time that could increase the risk of accidents to unacceptable levels.

This methodology has not been tested in a real-life railway application.

6.2.12 Prediction, Risk planning & Trouble-shooting

As part of good risk management practice, risk reduction measures introduced for specific risks or contributors to accidents are evaluated to assess how well they perform. Safety performance indicators can provide evidence of the condition of the railways with regards to safety goals being met or progresses towards targets and can be very useful tools to inform and justify the allocation of resources. The use of leading and lagging indicators in analysing the effectiveness of protective measures are simple and efficient methods that define, measure, monitor and inform accident precursors and safety performance. These protective risk reduction measures help assess the trend of incidents and subsequently predict the outcome of events.

Leading indicators are input-based information that have an indirect relationship to the risk reduction objective and can influence lagging indicators by measuring and tracking performance before an accident or incident occurs. Examples of leading indicators are increased frequency of signal overruns indicating imminent accident if not avoided. Number of recent wrong side door openings on the automatic train door system, an incident that will immediately require response or action to eliminate further escalation of the incident. Others are increased incidents of improper train berthing and the root cause could be track or train-related braking or complaints per 1,000,000 passengers. Other leading indicators such as number of passengers during peak periods or increasing number of passengers compared against overcrowding can help determine platform related incidents and subsequent protection measures to reduce the risks.

Similarly, lagging indicators are also effective measures for protecting against the risk of further propagation of an incident or accident. These are outcome related measures of safety performance directly related to the risk reduction objective. Lagging indicators measuring the number of preventable accidents per 1,000,000 kilometres provide information post-accident that facilitates protection-planning programmes.

Figure 43: Leading and Lagging indicators in risk reduction

RSSB (2011) evaluates the effectiveness and suitability of Safety Performance Indicators (SPI) used on Great Britain rail industry. The study ranks the SPIs in terms of maturity for specific applications. In this study on safety performance indicators used in the railway industry, definition of leading indicators proved problematic. The study states that no two definitions found were the same. The discrepancies in defining leading indicators results in certain circumstances an indicator such as signal passed at danger (SPADs) could be considered either leading or lagging. In order to eliminate this difficulty, the study defines leading indicators as the 'activity' indicator and lagging indicator as the 'outcome indicator'.

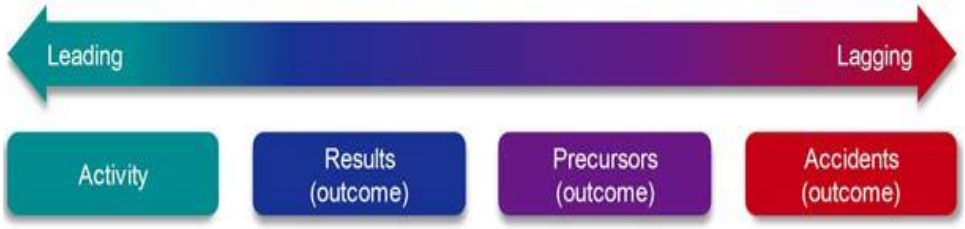


Figure 44: Safety Performance Indicators (adapted from RSSB 2011)

The study also identified that the fundamental flaw in the use and reliance on conventional on failure and accident data to monitor railway safety performance is that improvements or modifications can only be determined after an incident or accident has occurred.

Examples of current methodologies and technologies used for collecting accident data, reporting accidents, supporting accident investigations and periodic assessment of the performance of prevention or protection measures include:

1. Passenger Safety Indicator (PSI)

2. Train accident risk data from Precursor Indicator Model (PIM)
3. Safety Management Information System (SMIS)
4. Common Safety Indicators (CSI)
5. Transport Availability Infrastructure and Logistics System (TRAIL)
6. Service Contract Performance Database (CuPID)

6.3 Costs Associated with Implementing the Separate Protective Methods

Protective measures in general are associated with smaller capital costs compared to the preventive risk reduction measures. This is also demonstrated in the analysis of the magnitude of risk reduction against the cost of implementing protective measures. The costs of implementing individual protective measures with a positive impact on risk reduction are often shown to be relatively low when compared with preventive risk reduction measures.

These are illustrated below for each accident – Derailment, Platform Train Interface/Incidents and Collision between trains. The analysis assumes that the contributions to each accident as identified provide a comprehensive coverage of the primary risk scenarios. The distributions of contributions to the accidents are heavily dependent on recommendations and data from previous (internal) safety studies.

The chart depicts the cost of protective risk reduction measures and the risk reduction achieved. The data used for the chart illustration does not consider the negative values from two risk-reduction measures proposed for reducing the risk of 'Passenger falls between cars':

1. Introduction of new trains with open walkthrough cars
2. Introduction of new trains to reduce overcrowding

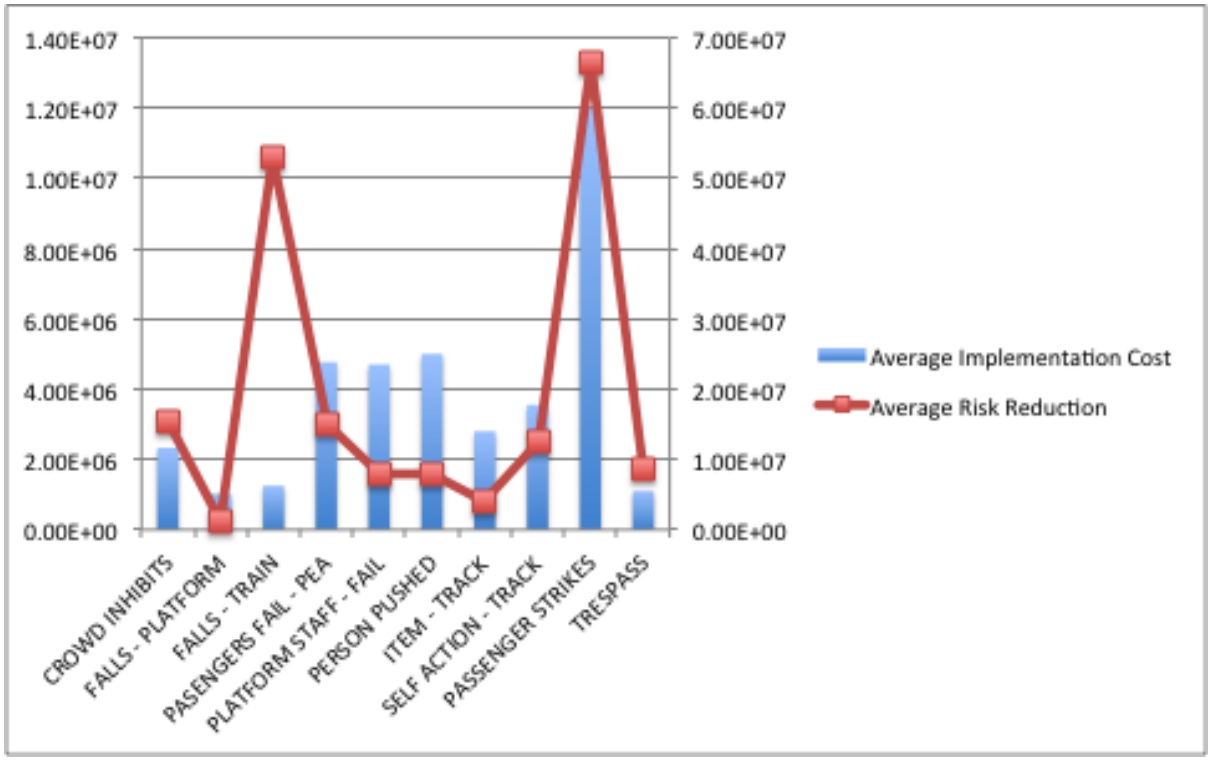


Figure 45: Effect of protective risk reduction measures on PTI

Figure 45 presents Platform Train Interface (platform-only) accident cost data analysis. The data presents the representative sample of key contributors to the major accident hazard, PTI. It highlights important features or trends that must be noted for any supporting decisions for selecting risk reduction measures. Let us consider risk reduction for 'falls from train to the platform' (FALLS-TRAIN), the chart shows the magnitude of risk reduction (in £) that can be achieved at a substantially low cost. This typically represents the risk reduction achievable eliminating gaps between the train and the platforms via gap fillers. Other protective risk reduction measures considered include addressing the causes and effect of illnesses on the trains. Options for reducing the risk of 'falls from train to platform' at a relatively low cost could also include signage and warnings; stair nose marking; crowd control; on-train supervision and additional platform lighting.

In the case of 'person pushed from platform' (PERSON-PUSHED), the average implementation cost is significantly larger than the average risk reduction achieved. In current practice, an ALARP and business case can be made for introducing other protective risk reduction measures such as designing and building anti-suicide pits instead of the generic platform staff support. Alternatives to the risk reduction measures identified in this study will have to be further identified to make a case for selection and implementation.

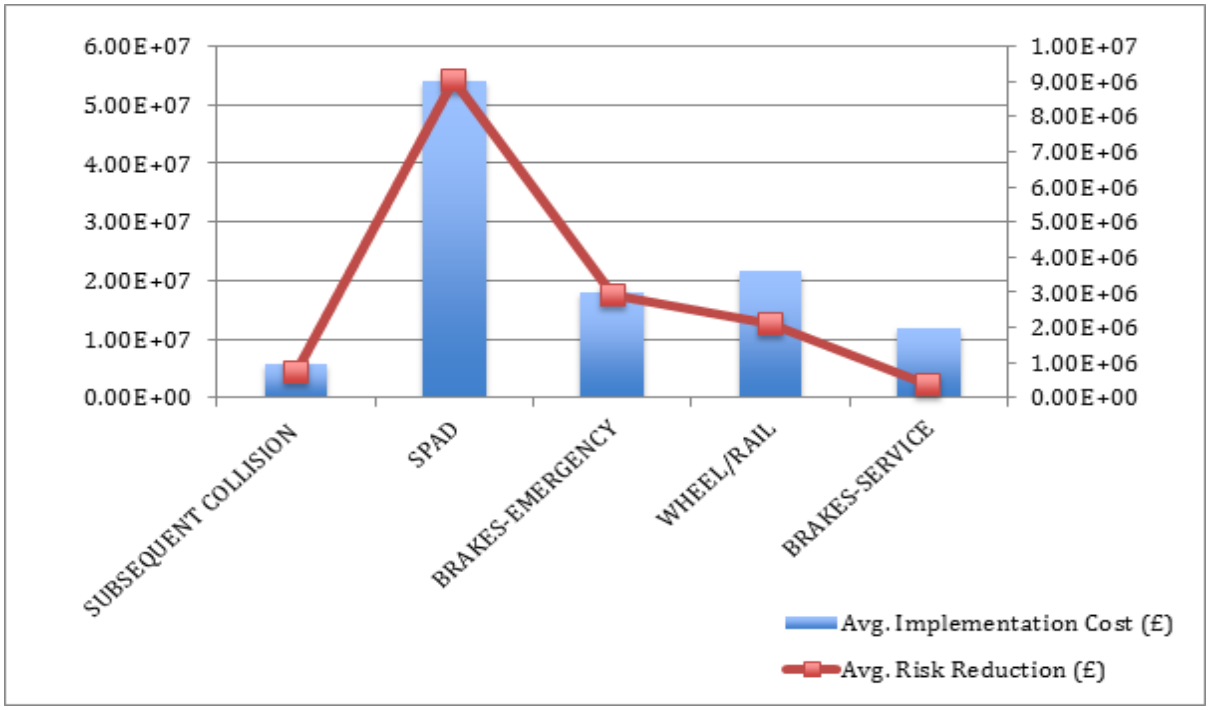


Figure 46: Effect of protective risk reduction measures on Collision Between Trains

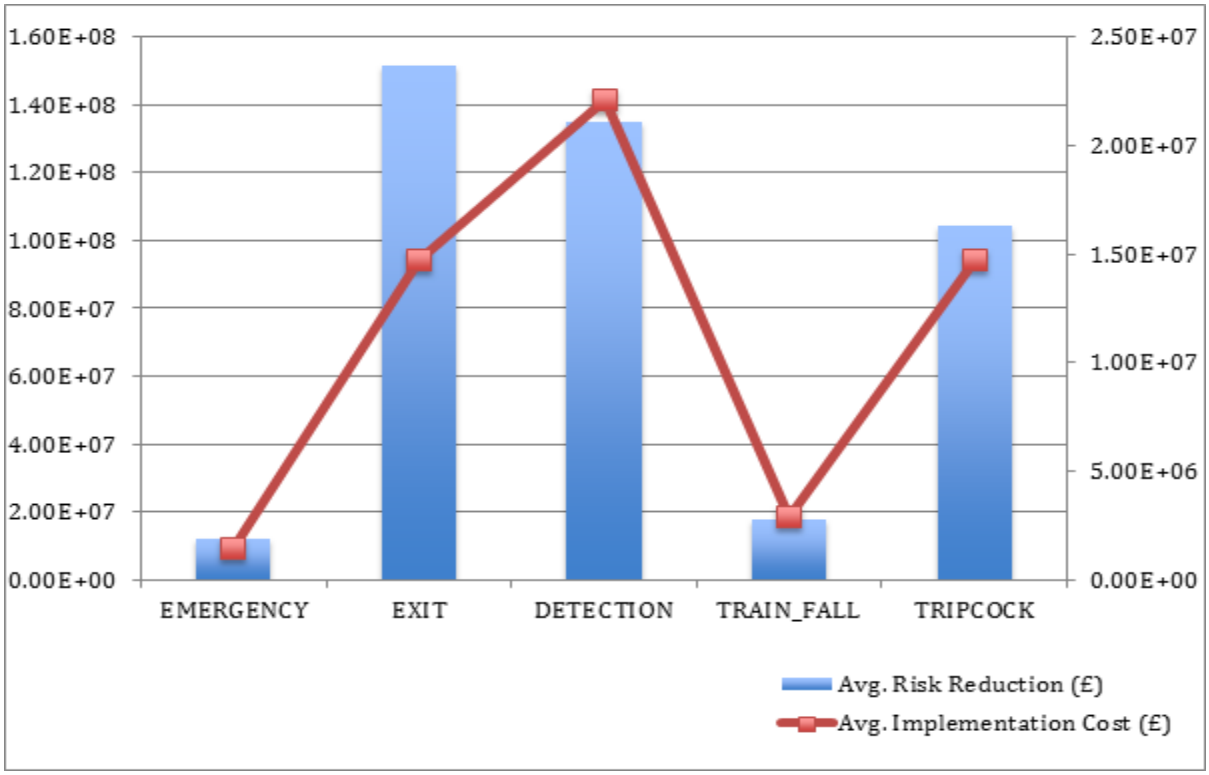


Figure 47: Effect of protective risk reduction measures on Derailment

For collision Between Trains, Figure 47 focuses on five major contributors – accidents as a result of Subsequent Collision, SPAD, Emergency Braking, Wheel-Rail interface and Service Brakes. The chart denotes alignment with safety and business cases for collision accidents. The ALARP case can be easier

made as the average cost of reduced risk is within the cost of measures considered. Figure 47 however shows that one can spend less to achieve more for the protection option 'emergency exits' (EXIT) subsequent to a derailment accident.

The above does not consider dependencies and effective risk reduction from possible combinations of these measures.

6.4 Removed Risk Associated with the Protective Methods

Similar to the information on preventive risk reduction measures provided in Section 5.3, Tables 16, 17 and 18 present details regarding the protective risk reduction measures and the corresponding risk reduction applications. These risk reduction applications are related to the typical contributors to the 'Major Accident Hazards' or fault tree 'Top Events'. In line with the scope of this study, Collision Between Trains, Platform Train Incidents and Derailment accidents only are detailed.

Table 16: Protective Risk Reduction Measures – Collision Between Trains

Protective Risk Reduction Measures	Risk Contributor (Collision Between Trains)
On-board sanding	**Service Brake Failure**
Vegetation management programme - leaf fall (autumn season specific challenge)	**Poor Wheel/Rail Friction**
Fitting of wheel slip protection or Adhesion improvers	
Emergency timetable - contingency plan for dealing with severe disruption (production of emergency timetables and dissemination of timetable information to all personnel especially operational personnel following an accident)	**Driver Passed Signal at Danger (SPAD)**
Crash worthiness and vehicle interior	
Speed restrictions (Adhesion)	
Precautions, procedural modifications and subsequently, driver training for running with isolated emergency brakes	**Emergency Brakes Fail to Function**
Emergency accident/incident plans	**Collision with another train subsequent to a collision**
Training for drivers and incident centre personnel	
Training for local emergency medical team on train accidents/incidents	
Audible warning systems - trains	

Table 17: Protective Risk Reduction Measures – Platform Train Incidents

Protective Risk Reduction Measures	Risk Contributor (Platform Train Incidents – Platform)
Additional support from platform supervisors	**Crowded platform inhibits driver's view (crowding)** **Person pushed from platform** **Person retrieving item from platform**
Audible warnings on platform (Improvements to passenger display screens and public address systems)	
Emergency plans - incident management plan	
Increased use of slip, trip and fall toolkit	**Passenger falls from platform**
Signage/Warnings and car door alarms (Trains)	
Anti-suicide pits on track area	
Platform staff support (incident control - drag and pull) - Same as above Additional support from platform supervisors	
Review of incidents of passengers being taken ill on trains to establish common causes and develop plans to reduce the numbers of such incidents	**Falls onto the platform from train**
Gap fillers - Platform rubber	
Deployment of train co-ordinators train-cars	
Introduction of Sensitive door system	**Train passengers fail to activate Passenger Emergency Alarm (PEA) within station limits**
Passenger Emergency Alarms locations reviewed and relocated	
OPO CCTV (Same as 'Introduction of improved OPO CCTV systems' above)	
Speed restrictions - enforcement of speed restriction on platform areas	**Platform staff unable to stop train before it moves off with trapped passenger**
Crowd control	
Audible warnings on platform	
Under-platform lighting	**Person retrieving item from track**
Audible warning systems - platform (station area) - Same as 'Audible warnings on platform…' above	**Person on track due to self-action (miscellaneous)**
Audible warning systems - trains	
Crowd control station platform area (Same as 'Crowd control') above	
Speed restrictions - aerodynamic effect of train on passengers on platform (Same as 'Speed Restrictions - enforcement of speed restriction on platform areas' above)	
OPO CCTV (Same as 'Introduction of improved OPO CCTV systems' above)	**Passenger strikes/falls against train**
Audible warning systems - trains (used following track trespass)	**Trespass on track in station area**
Additional station/platform staff training (See 'Station Master/personnel training' above)	

Table 18: Protective Risk Reduction Measures – Derailment

Protective Risk Reduction Measures	Risk Contributor (Derailment)
Structural re-enforcements - bridges, embankments	**Train falls down an embankment or from a bridge after a fast derailment**
Reduced traffic on bridge/structure	
Repositioning of tripcocks - standard requirement is tripcock positioning 1.5m from front of train	**Trip-cock fails to activate brakes**
Introduce injury prevention initiatives e.g. booklets, DVDs and staff briefings	
Introduction of (improved) shunting policy	**Loss of train detection – Train fails to shunt track circuit**
Trains fitted with incident response kits and additional training for staff to act as quickly as possible in emergency situations	
Crowd control	**Involuntary exit**
Fire and rescue services	
Paramedics/medical units (availability of staff trained for train accident scenarios)	
Seat belts restraining passengers to their seat	
Emergency Door Release	**Emergency exit**
Trip systems to isolate or de-energise traction power	
Emergency lighting and signage (illumination of Emergency Door Release mechanisms in passenger vehicles)	
Provision of hammers for emergency exit	
Seat design to minimise passenger injury	

The success of any one or combination of the risk contributors potentially leads to accidents with resultant fatalities/injuries. The protective risk reduction measures are used individually or in combination to effectively remove or reduce the effect of the risk contributors. The risk reduction measures presented in the tables above are not in any way exhaustive but representative of the primary measures used in the overall study. Other risk reduction measures are detailed in the following sections providing a complete with the decision support strategy proposed in Chapter 7.

6.5 Constraints and Considerations in Selecting Protective Risk-Reduction Measures

The general guidance for selecting protective risk reduction measures is 'what you don't know can hurt you…' Protection measures are most effective in application to high uncertainty and unexpected events – the 'black swan' effect (Taleb, 2007).

Even in an industry with a long history of accidents, a good record of consequences and potential escalation of accidents, if proper protection measures are non-existent, the adoption of the 'prevention is

the best cure' philosophy provides a false sense of the actual state of operational risks. When considered, protective measures are typically an afterthought. On some major capital projects, the heavy-loaded investments in preventive measures drain the budget before any protective measures are even considered. In such cases, optimisation or intense rationalisation of measures to implement subsequent to a failure of the high-tech signalling system, as used in this example, becomes essential. However by the time the project team get to this realisation, the high tech signalling system is already contracted out or secured/procured. Decision support techniques (rational and optimisation methods) that remove this loop-hole in current practice is outline in Chapter 7 and presented in by Weli and Todinov (2013a); Weli and Todinov (2013b); Todinov and Weli (2013).

Similar to the selection of preventive risk reduction measures, training, monitoring and supervision are essential for effective implementation of protective risk reduction measures. An example is the selection of a protective risk reduction measure such as introduction of One-Person-Operated Closed Circuit Television CCTV (OPO-CCTV). The OPO-CCTV is situated within the cab for a driver to have complete view of the platform and surroundings. The measure provides significant risk reduction and as a result minimises the risk, amongst others, of a passenger sustaining further injuries after falling between the train and the platform. By using of the OPO-CCTV, the driver is provided with better awareness of the situation and will not start or move the train. This measure for reducing risk does not preclude that the driver and platform staff require training on actions to take in the event of a passenger fall. The driver still needs to be aware and monitor the screens with possible help from platform staff and other passengers. Risk assessments undertaken for the use of the in-cab CCTV also suggests that platform supervision must supplement the use of the OPO-CCTV system.

In Section 6.2.10, degraded operations as a risk reduction principle was listed as effective for risk reduction particularly in cases where no sounder alternative exists. Following accidents, incidents or failures on the railways such as SPADs, buckled rail or signal failure, the degraded mode of operation is usually the only feasible alternative as trains may need to carry on to stabling depots, reduce congestion or reduce the consequences from lack of ventilation if trains are stuck in the tunnel. However, considerable amount of care is needed to ensure effective application such as prior scenario safety assessments, work-around procedures and occasional training irrespective of the frequency of the accidents.

On the railways, the measures generally classified as protective (also see classification in appendices) are relatively cheaper and take less time to implement. Nevertheless, the heavier burden of cost is in ensuring the maintenance and continuity of the measures. A typical example to illustrate this cost continuity for two measures that provide similar risk reduction at different costs is the platform

emergency stop plunger (PESP) and the train driver. The PESP will require significant investment for initial procurement, installation, testing and handover/commissioning. However, the occasional inspections and annual maintenance checks are low compared to the recruitment/salary of a train driver at a lower cost to the PESP and increased cost of regular relevant training and exercises required to keep the train driver updated and efficient.

6.6 Effective Methodology for Selection of Preventive or Protective

The primary objective of the proposed methodology and strategy is to find a solution to the flaws in the existing practice and in so doing, to develop a comprehensive and structured framework for effective risk reduction. This task does not come without its own challenges. These are also highlighted and resolved. The main challenge is the development of a framework with a structured case that presents the decision maker with a great degree of confidence that effective risk reduction measures are considered – this includes correct application of risk reduction measures and at a reasonable cost. Setting out on this work, some careful thought was put to the typical questions that inundate a decision-maker on the application of effective risk reduction measures. The questions are comprehensive, albeit not exhaustive and in no particular order. The quest is presented as an overview of some of the fundamental challenges to applying risk reduction measures which have not been addressed in current practice. These include:

- In what cases are preventive or protective measures applied for cost effective risk reduction?
- What risk reduction measures do we invest in and how is this achieved for particular railway accidents and accident scenarios?
- Assuming we have identified and know the risks or contributors to a major accident, is the introduction and implementation of only preventive risk reducing measures sufficient to reduce the risk as low as reasonably practicable?
- In cases where the risk cannot be easily quantified, how are risk reduction measures applied?
- With varying degrees of uncertainty in data, what methods are in place to reduce the under-estimation or over-estimation of magnitude of risk reduction and cost effectiveness used in the economic analysis for selecting risk reduction measures?
- In new railway developments with associated scrutiny on costs, is it worth more investment in measures that prevent the risk or protect against the risks of accidents?
- What is the most effective way of allocating budgets - how are the preventive and protective risk reduction measures for a particular risk distributed or allocated?

- How are risk reduction measures which act in parallel to other measures determined and what is the contribution of these parallel measures to the overall risk reduction objective?
- In marginal reduction cases, mostly cases encountered on the railways, how could preventive or protective measures be appropriately employed?
- What important cost considerations drive the decisions on preventive or protective measures?

In view of the above and limited research work existing to address these, it can be surmised that the fundamental requirements of applying risk reduction measures can be achieved if a comprehensive decision support system developed specifically for railway risk reduction applications aims to meet two primary objectives:

- Effective application of preventive or protection measures
- Effective combination/balance of preventive or protective measures

The scope of the methodology is not limited to solutions to the above but attempts to extend the understanding and application of risk reduction measures on the railways.

6.7 Classification of Risk Reduction Measures (Preventive and Protective)

A simple distinction of any given set of measures as preventive or protective based on railway risk reduction specific application requirements can be achieved by evaluating their specific application properties against the generic principles of risk reduction. This is based on the comprehensive evaluation of preventive and protective measures presented in Chapters 5 and 6.

Given a set of risk reduction measures, the qualitative effectiveness of each of the risk reduction measures is evaluated by applying the generic risk reduction principles. A comprehensive understanding of the functional limitations and capabilities of each risk reduction measure in the particular risk scenario can provide evidence for assessing its benefits and potential for use in an application.

The associated limitations and capabilities are based on an assessment against the basic principles of risk reduction and can be evaluated against other risk reduction measures with estimated risk reduction and associated costs. The limitations highlight the application constraints of the risk reduction measure and provide a means for considering parallel risk reduction measures to supplement or support the risk reduction measure at a reasonable cost.

The evaluation of risk reduction measures using both preventive and protective risk reduction principles is in line with assertions made in previous sections of this work, that risk reducing measures potentially

exhibit attributes for reducing the likelihood of an accident or the consequence in the event of an accident or both.

Let us consider the unambiguous classification of SPAD risk reduction measures that effectively supports a decision-maker by effectively minimising the risk of selecting an incorrect measure. The decision-maker is provided with a means of assessing the properties of each measure, based on already introduced engineering risk reduction principles. This helps assure that for any specific risk reduction application, the properties that dominate subsequently influence decisions made on its use as a preventive or protective measure. The characteristics of 14 risk reduction measures are assessed and presented in the simplified matrix, Table 19 and Table 20 below.

Table 19: Functional capability (preventive) of risk reduction measures for SPAD risks

Major Accident	Contributor	Risk Reduction Measures	Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Sensitivity to SPF	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise human errors
Collision	SPAD (Including signal over-runs)	Automatic train Operation	•	•	•			•						•
		Overlap extension						•						
		SPAD incident response system												
		Signalling modifications				•	•		•					
		Speed restrictions									•	•		
		Driver and Line Controller training												•
		Wheel-side protection systems					•			•				
		Trip-cock positions relocated		•										

Major Accident	Contributor	Risk Reduction Measures	Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Sensitivity to SPF	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise human errors
		Speed control systems	•	•										•
		Brake control systems	•	•										•
		In-cab design modifications							•					•
		Train Protection and Warning Systems	•	•	•	•								•
		Testing and maintenance					•						•	
		Emergency timetable										•		•

Table 20: Functional (protective) capability of risk reduction measures for SPAD risks

Major Accident	Contributor	Risk Reduction Measures	Protective Barriers	Damage Arrestors	Blocking Pathways	Using Fail-safe devices	Introducing weak links	Delaying deterioration	Exposure time/duration	Vulnerability of targets	Emergency systems	Degraded operations	Failure indicators	Prediction, Risk Planning, Troubleshooting
Collision	SPAD (Including signal over-runs)	Automatic train Operation	•			•							•	
		Overlap extension												
		SPAD incident response system			•			•	•	•	•			
		Signalling modifications				•								
		Speed restrictions	•					•	•	•	•			

Major Accident	Contributor	Risk Reduction Measures	Protective Barriers	Damage Arrestors	Blocking Pathways	Using Fail-safe devices	Introducing weak links	Delaying deterioration	Exposure time/duration	Vulnerability of targets	Emergency systems	Degraded operations	Failure indicators	Prediction, Risk Planning, Troubleshooting
		Driver and Line Controller training										•		•
		Wheel-side protection systems												
		Trip-cock positions relocated												
		Speed control systems	•			•								
		Brake control systems	•		•	•								
		In-cab design modifications					•	•		•				
		Train Protection and Warning Systems	•			•							•	
		Testing and maintenance					•						•	
		Emergency timetable	•					•	•	•	•	•		•

The classification of each risk reduction measure as either preventive or protective is simplified by assessing the specific application capabilities and highlights the predominant attributes of each risk reduction measure as:

1. Preventive – Automatic Train Operation, Signalling Modifications, Wheel-slide protection systems, Relocating Trip-cock positions, Speed Control system, Extending/improving testing and maintenance regimes or scope;
2. Protective – SPAD incident response, Speed Restrictions, Driver and Line Controller Training, Emergency timetable
3. Preventive and Protective (Dual) – In-cab design, Brake control system

Using this approach, Appendix A provides a complete data set of distinctly classified risk reduction measures for 220 different risk reduction measures identified for a major UK railway renewal project.

Chapter 7 Considerations and alternatives for Rational and Optimal Budget allocation to achieve a Maximum Risk Reduction

A thorough understanding of the elements of risk is a prerequisite to appropriate comparisons related to the effectiveness of measures minimising risks As Low As Reasonably Practicable (ALARP). Risk evaluation and reduction derived from first principles eliminates the ambiguity currently existing in current practice in railway safety cases. Reviews of railway operators' safety cases indicate that necessary work needs to be undertaken to present risks assessment and risk reduction as an integrated activity and presented in safety reports as such – traceable and easily appreciated.

In view of the above and the very limited research work existing to address these, it can be surmised that as a minimum, the fundamental requirements of applying risk reduction measures can be achieved if decision support systems specifically developed for railway risk reduction aims to meet two primary objectives:

1. Cost effective application of risk reduction measures
2. Cost effective combination/balance of preventive and protective measures

The scope of the thesis is not limited to solutions to the above but to extend the understanding and application of risk reduction measures on the railways (as provided in Chapters 5 & 6). The final goal is to maximise risk reduction when a fixed budget is the major constraint. Considering this goal, chapter 7 uses novel concepts such as the Cost of Failure concept and proven system engineering methods to address challenges to achieving maximum risk reduction identified in preceding chapters. Comprehensive and structured practical solutions to the current misguided practices are also submitted.

In this chapter, the rational approach to maximum risk reduction in the railway industry further presents:

- The application of the key risk reduction principles introduced in chapters 5 and 6 into the existing industry accepted method for selecting of measures and presents a simplified, systematic and verifiable options selection approach
- Organisational challenges of implementing measures selected and addresses these by presenting:
    - The Risk Reduction Readiness Model (R^3M)
    - Contracts and Supply Chain Risk Reduction Model
    - D-O-P-T (Design-Operational-Procedural-Technical) classification. This is a categorisation of the risk reduction measures to eliminate the gaps between the initiation and implementation phases of the risk reduction lifecycle.

7.1 Risk Concepts, Considerations and Methods for rational and optimal risk reduction

It is important to define the concepts; constraints and variables; and methods considered that help with the development of the new approach. These are summarised in the subsequent sub-sections. Other concepts or definitions used are adequately referenced to previous sections where originally introduced.

7.1.1 ALARP Concept

The Health and Safety at Work Act (1974) stipulates that expenditure to reduce hazards must be incurred up to the point where the remaining risk is 'as low as reasonably practicable' (ALARP). The HSE framework for the tolerability of risk defined in HSE (2001c) and adopted on the UK railways is illustrated using the triangle in Figure 48. The value of preventing a fatality for 2012 was calculated by the Department for Transport (DfT) guidance to be VPF_{2012} = £1,653,000. This value is used in quantitative analysis to aid decision-making and its use will be maintained for the case studies and examples in this thesis.

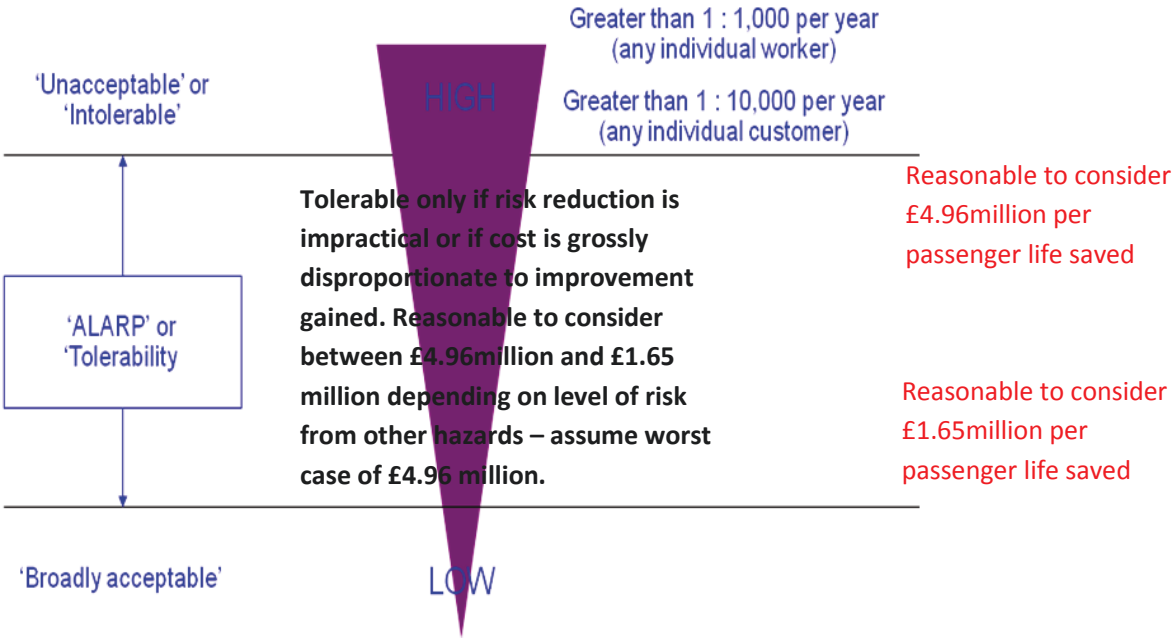


Figure 48: ALARP Triangle and Tolerability of Risk

The ALARP triangle above is calibrated against most railway safety standards in the UK. In general, an aggregate risk for a system under review below 0.001 fatalities per annum is considered broadly acceptable/tolerable. Above 1 in 104 risk to the individual is considered intolerable. The risk reduction benefit for individual risks between 1 in 105 and 1 in 104 is taken as £4.96million per life saved and for other areas of the ALARP region to be £1.65million per life saved. Expenditure on risk reduction measures

to minimise the occurrence of incidents, which could lead to loss of life, injury, or damage to assets is expressed in money metrics.

Cost-of-failure concept

The direct and accurate application of a risk reduction measure to specific accident or risk scenarios is essential to cost effective risk management. As the risk reduction capability of a measure or combination of measures increases, the likelihood of failure or consequences decreases.

Using the cost-of-failure *(CoF)* concept introduced in Section 2.4, a risk reduction strategy can be developed that reduces the risk of railway accidents (Todinov, 2003).
Applying $\mathrm{K} = \mathrm{pf} * \mathrm{C}$, then;

$$\mathrm{pf} = \mathrm{K}/\mathrm{C} \qquad (7.1)$$

If Kmax is the maximum acceptable risk of failure and pfmax is the corresponding maximum acceptable probability of failure, equation (7.1) is given as:

$$\mathrm{pfmax} = \mathrm{Kmax}/\mathrm{C} \qquad (7.2)$$

The cost-of failure concept provides that for reducing the risk of failure, the probability of failure must obey the inequality:

$$\mathrm{pf} \leq \mathrm{Kmax}/\mathrm{C} \qquad (7.3)$$

This means that whenever the probability of failure is $\mathrm{pf} \leq \mathrm{pfmax}$, the risk of failure is reduced below Kmax, the maximum tolerable risk. For the minimum reliability of the system which reduces the risk level below Kmax we get:

$$\mathrm{Rmin} = 1 - \mathrm{Kmax}/\mathrm{C} \qquad (7.4)$$

This expresses the principle of the risk-based design formulated in (Todinov 2007): for a specified level of tolerable risk Kmax, systems whose failures are associated with large cost C should be designed to a higher reliability level compared to systems whose failures are associated with smaller cost. At the same time, for the same minimum reliability of the system a risk-reduction measure limiting the cost of failure automatically reduces the level of risk Kmax.

7.1.2 Allocation and Management considerations for Risk Reduction

There is a range of events that result in accidents and in some cases; there is an even broader range of associated risk reduction measures and combination of measures. It is important that these measures and varying combinations for the specific risk reduction application are efficiently utilised throughout the

operational period. An efficient method for managing specific application safety risk reduction measures is by clearly delineating and categorising the measures for appropriate allocation to the correct sections of the organisation.

However, the categorisation of risk reduction measures on the railways as an integral part of effective risk management is hardly in existence. It is an underestimated area that requires further development. In other industries where risks drive investments and business decisions, integrating risk reduction with operational categorisation is a core requirement. Marshal (2001) and Bessis (2002) provide comprehensive views of operational risks, defining these as event risks and argue that to effectively handle risks of potential losses, categorisation of events will serve as a receptacle for accident data gathering on frequencies and costs. A tentative categorisation of event risks is presented under:

- People
- Processes
- Technical
- Systems

In the absence of efficient tracking and accident reporting systems that directly categorise risk reduction measures and their functional capabilities for reducing the likelihood of an accident and consequences, **vital risk reduction measures are ignored** and therefore do not trigger any requirement for their incorporation. This practice could have potentially catastrophic consequences.

The clear outline in roles and responsibilities within the risk reduction context ensures that resources (finances, technical expertise, information, systems/equipment, medical facilities etc.) necessary for implementing the measures are available and used to good effect.

The effective introduction of these risk-reduction measures must take into account the possible duplication of effort and consider whether the organisation or specific departments within an organisation could be better placed. This fundamental requirement for any effective risk reduction must be applied to the whole life of the project or system. The inter-relationships between departments forming part of a railway risk reduction operation can serve as the baseline structure for developing measured strategies for accident prevention and protection. Throughout the project or system lifecycle, the clearly defined inter-relationships on reducing any particular risk ensures that the railway operations are able to take advantage of the many technical resources that exist within the organisation. Any categorisation employed must also specifically apply to the typical railway organisational structure in order to achieve the full benefits of the risk reduction measures over the usage period. This is facilitated

by correctly associating the typical functions of a risk-reduction measure to the typical responsibilities within an infrastructure operator.

7.1.3 Systems Engineering (SE) method to effective risk reduction

By definition, the system engineering approach to risk management must ensure effective risk reduction for any major railway renewal or developmental project. A considerable amount of effort is expended on planning, evaluation and management of potential risks prior to the selection of risk-reduction options. A process of cost and benefit evaluation would normally precede such selection. In practice, the selection of risk-reduction options is constrained by fixed budgets. The greatest challenges of introducing and effectively managing risk-reduction options are:

1. Novelty of the option;
2. Complexity of each risk reduction option;
3. Integration issues.

The integration issues include:

- the interaction between subsystems to achieve risk reduction;
- the correlation and interaction among the risk reduction options; and
- the correlation and interaction between the risk-reduction options and the environment.

By considering these interactions as important factors in the risk reduction exercise, the safety and business case claims for risk removed and their cost effectiveness can be substantiated and further enhanced to support their acceptance and successful implementation.

By revealing the complex interrelationships between the risk reduction options, the gap between risk evaluation, options selection and implementation (i.e. costs, people, process and equipment) can be effectively narrowed. The adoption of the systems approach provides coordination between people, processes and equipment at the implementation phase, where the organisation plays a crucial role in the risk management process. In this sense, **the systems approach provides a bridge to the organisation structure**. A comprehensive understanding of the limitations and strengths of each option for the specific application is a prerequisite for effective overall risk reduction (comprehensively addressed in Chapters 5 and 6). For major railway projects with multiple risk reduction options, the key to effective risk reduction lies in the successful integration of the available options.

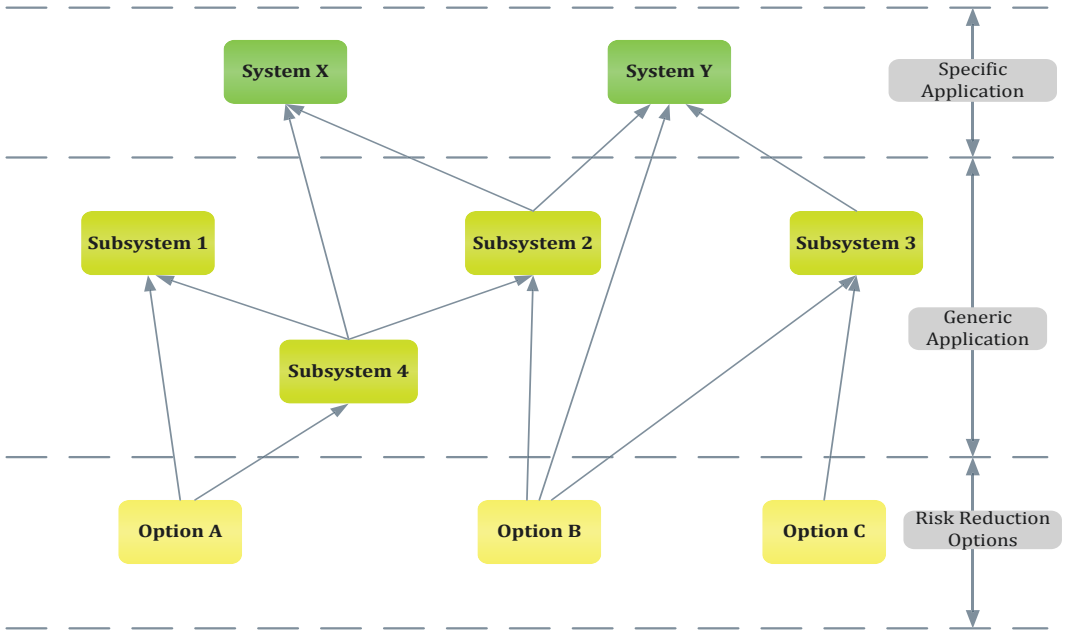


Figure 49: Systems engineering approach to risk reduction

7.2 Rational approach to risk reduction in the railway industry

The classic expression for risk (Vose, 2000), presented in Section 2.4 includes ρ - the probability of risk actualisation and C - the consequence or cost as a result of the risk being realised. Realisation of the risk on the railways is any incident or accident with a negative impact. Most railway applications of this basic equation, similar to other safety-critical industries, define that risk is a combination of the probability of occurrence, C and the probability of the harm occurring, ρ. Furthermore, ρ is also developed into three primary parts:

- The likelihood of the risk occurring, σ
- The probability of not reducing the harm, θ
- The frequency of operations/duration of exposure to the hazard, ω

Applying these three parts to the basic equation gives:

$$K = \sigma\theta\omega C \qquad (7.5)$$

Estimations of the risk take into account past accident data and if these are unavailable, engineering expert judgement is employed. Severity or consequence following an accident are considered by taking into account the gravity of injuries and are generally classified as minor, major or fatal. The likelihood of the risk occurring is estimated using reliability data, accident history, and other statistical data. The probability of avoiding the harm introduces the human element to the assessment and the consideration

of the actions of personnel and passengers, i.e., how quickly the risk event can occur, awareness of the risk and response (and response times) by passengers or personnel. The frequency or duration of exposure to the hazard can be estimated by taking into consideration:

- Time spent in the danger zone
- Number of persons that must access the area
- Frequency of access or operations

Once the risk has been estimated and a risk reduction is required (i.e. intolerable risks are identified), risk reduction objectives are set and decisions on risk reduction measures are made and implemented. The railways use economic cost-benefit analysis and the ALARP approach to determine the best options to implement. Figure 50 shows the risk assessment and risk reduction selection process adopted, i.e. risk analysis, evaluation and management.

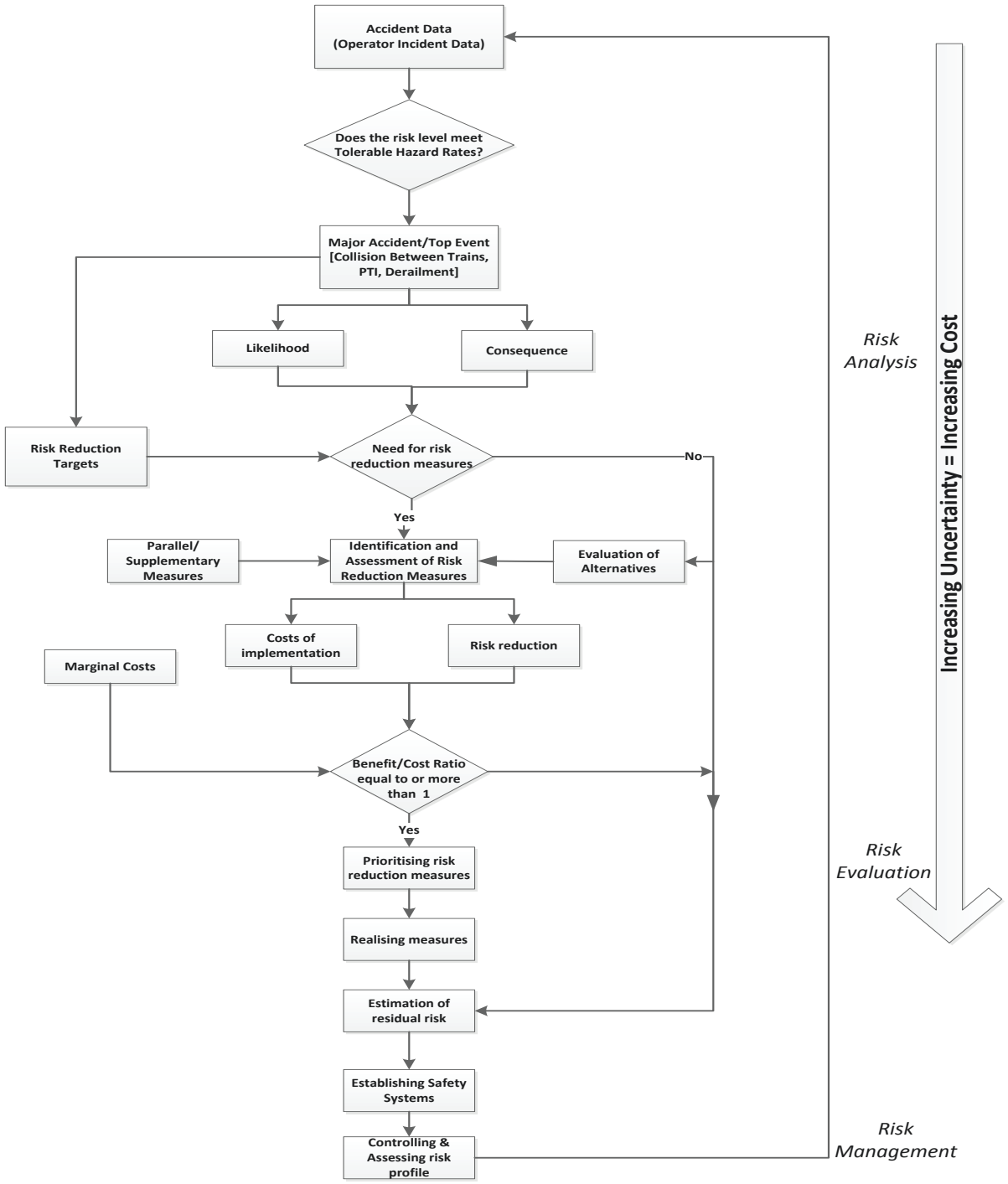


Figure 50: Selecting risk reduction measures (current railway safety method)

Considering that the accuracy of these parameters are currently heavily dependent on a robust and significant degree of accident or failure data, the case for uncertainty in the analysis increases. Weli and Todinov (2013a) establish that the results of the current approach have varying degrees of uncertainty and do not support the required minimum cost and effectiveness objective. This thesis demonstrates that the current conventional method for selecting risk reduction measures following the above risk

evaluation is limited in its ability to adequately support the overall risk management objective. In fact, this approach yields misleading results and incorrect risk reduction-related decisions.

One of the primary requirements for risk reduction in the railway industry and similar safety-critical industries is that measures applied to reduce risks must be verifiable. This is a major challenge for the existing methods with their critical dependence on accident risk data. Currently, no practical and verifiable alternative exists for this selection. Common sense suggests that the methodology must not be entirely dependent on historical accident data. A set of accident data is always associated with particular designs and conditions and cannot be entirely transferred to describe new designs and conditions. Accident frequencies relevant to old designs and conditions in general, cannot be extrapolated to new designs and conditions. Sensitivity analysis has been considered as a tool for preventing misleading results from risk analysis and subsequently from cost-benefit studies. However, sensitivity analysis methods have been shown to contribute to inaccuracies. Their limitations have been well documented in Cullen and Frey (1999); Menard (1995); Von Winterfeldt and Edwards (1986); Winer et al. (1991); Saltelli and Bolado (1998); Lindman (1974); Neter et al. (1996).

In view of the number of fundamental weaknesses in the existing railway industry practice, this section proposes a new decision support approach, based on sound, comprehensive and structured engineering principles for identifying and selecting risk reduction measures. The opportunity to make this major improvement in the current railway risk management practice is the focus of this work.

7.2.1 New approach based on fundamental, verifiable risk reduction principles

Figure 50 illustrates the existing approach that is used to support investment decision-making on risk reduction for a typical railway project (same as Figure 51). Figure 51 further highlights the area X, which shows that the cost-benefit approach to risk reduction is based on prioritising and selecting the risk reduction measures according to their cost-benefit ratio. The effectiveness of existing approaches and tools cannot be verified as they are heavily reliant on historical data, which are neither representative nor reliable for accident costs and risk-reduction benefits. Furthermore, the historical data are not valid for new designs and new conditions. These circumstances significantly increase ambiguity in decisions; reduce the level of confidence in the selected risk management procedures; and make it impossible to develop a robust case for the railway safety application.

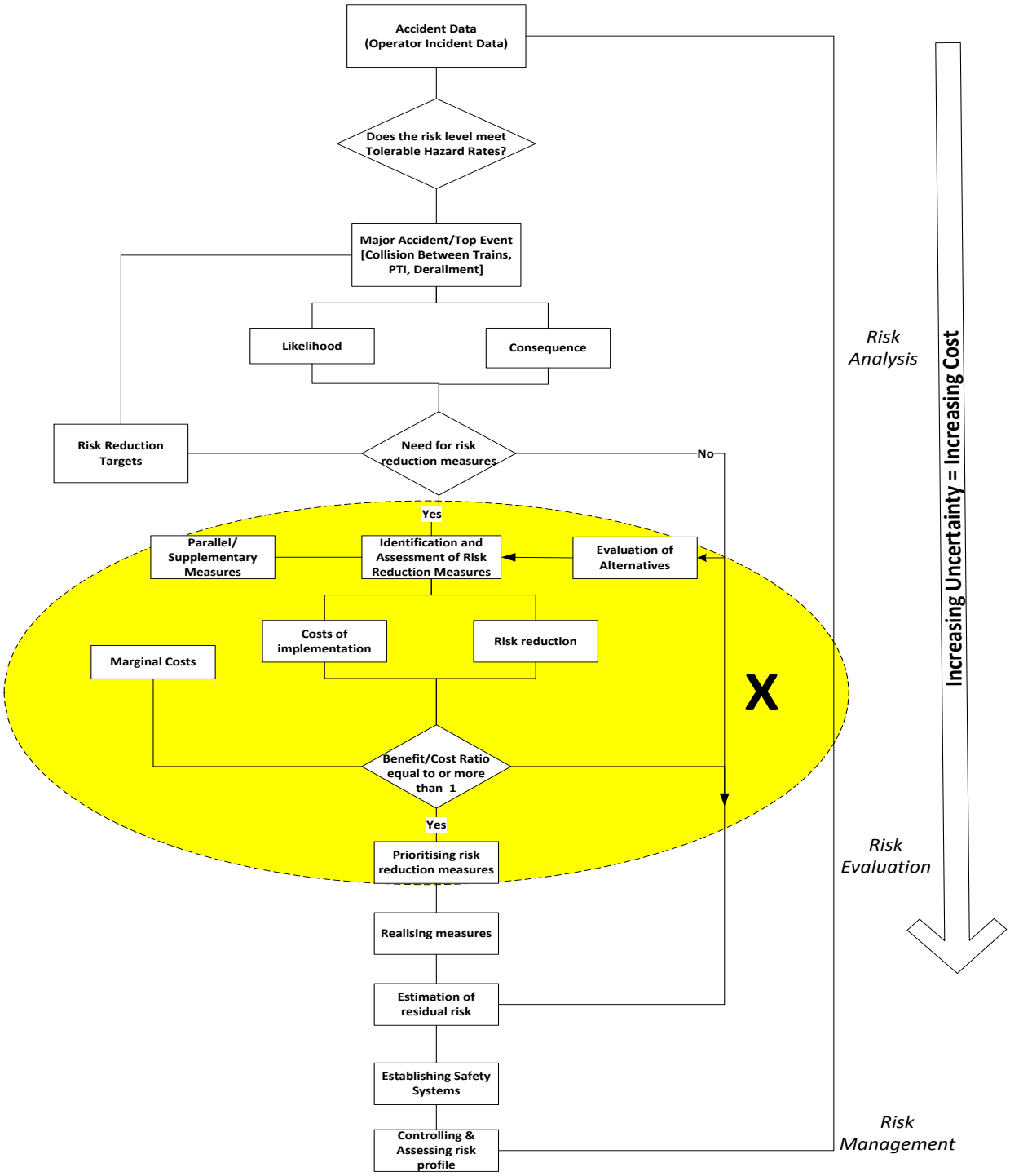


Figure 51: Selecting risk reduction measures (region X introduces incorrect decisions)

This focus of the new approach is to eliminate the inaccuracies introduced into selecting risk reduction measures within the highlighted region X.

By using a *'cost-of-failure' (CoF)* concept and the generic principles of risk reduction (Todinov, 2007) an appropriate set of generic risk-reduction principles can be formulated, specific to the railway industry, from which risk-reduction measures can be derived. Such measures reduce the likelihood of a railway

accident or its consequences in the event of the accident. Subsequently, the identified risk-reduction measures are assessed with regards to the amount of risk each of them removes and the cost of their implementation. Table 21 presents 24 key generic principles. They are referred to as 'preventive' if they reduce the likelihood of a railway accident or 'protective' if they reduce the consequences. Extensive details and work on the application of these principles are provided in Chapters 5 and 6.

Table 21: Key risk reduction principles (preventive and protective).

Principles for reducing the likelihood of an accident (Preventive)	**Principles for reducing the consequence of an accident (Protective)**
Built-in redundancy e.g. braking systems, route locking systems, position detection systems	**Protective barriers** e.g. thermal barriers as passive protective systems for risk reduction
Increased connectivity e.g. on-board train units.	**Delaying deterioration** e.g. refurbishments
Derating e.g. voltage alterations in track circuits for different operating temperatures	**Blocking pathways** through which accidents escalate e.g. platform emergency plungers
Reducing sensitivity to common cause failures e.g. design diversity in train control systems	**Introducing weak links** e.g. Crash Energy Management (CEM)
Minimising interfaces, complexities, weak links and connections e.g. use of closed communications networks	**Reducing the vulnerability of passengers** e.g. platform CCTV or OPO -CCTV for stuck at door or falls between train and platform
Simplification of operations e.g. use of software based systems to simplify application such as automating braking systems	**Use of fail-safe** devices in isolation techniques e.g. stick relays to de-energise track circuitry following an accident
Maintaining resistive forces and continuity of action e.g. wheel-slip and slide control	**Emergency response** e.g. emergency timetables, incident systems, first aid tool kit
Opposite effect modifications e.g. stressing track	**Degraded operations** e.g. speed restrictions
Operations frequency e.g. introducing trains into service to reduce overcrowding	**Damage arrestors e.g.** over-voltage or surge protection
Testing, inspections e.g. to detect latent faults	**Exposure time** e.g. crowd control
Reducing human errors e.g. training of drivers, controllers, in-cab designs.	**Failure indications** e.g. Automatic Warning System,
Voting systems reducing the likelihood of erroneous signals; interlocks preventing a wrong sequence of actions (e.g. controls and signalling systems)	**Prediction, risk planning and trouble-shooting** e.g. use of leading and lagging indicators in risk reduction

The region X is replaced with a well-defined and structured approach that replaces the highlighted activities. The proposed approach presented by Figure 52 is based on a comprehensive understanding of the functional capability of the risk reduction measures applied to specific railway risk scenarios. Chapters 5 and 6 outline these functional capabilities by illustrating the strengths and limitations of preventive and protective measures in applying the fundamental risk reduction principles to the railway industry.

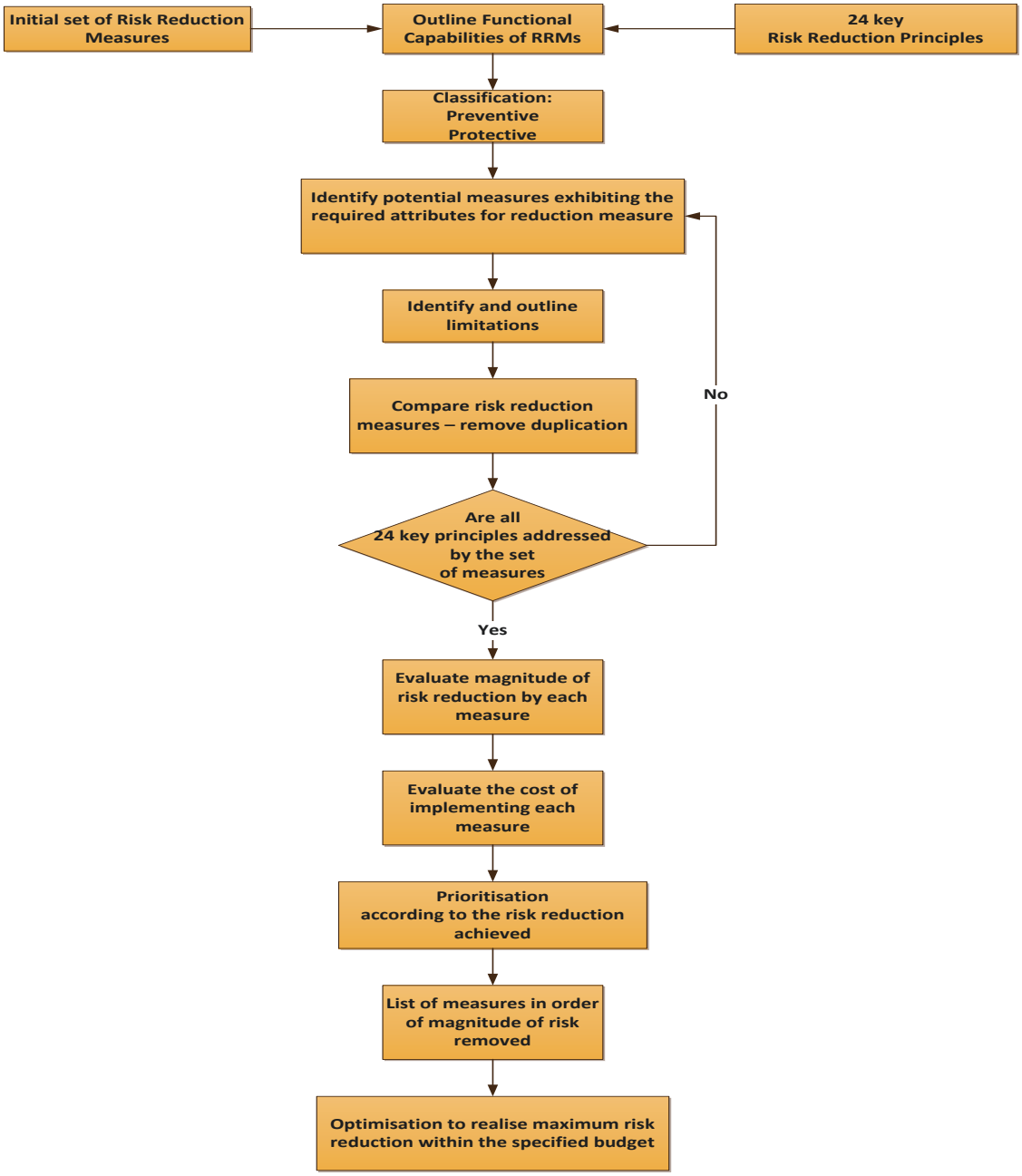


Figure 52: Simplified new risk assessment and options selection approach

The process starts with assigning risk reduction measures to the different risk contributors or risk scenarios resulting in a major railway accident. Using the 24 key risk reduction principles, the measures are classified according to their potential for reducing the likelihood of the accident (preventive measures) or reducing the consequence of an accident (protective measures). Each risk reduction measure is also assessed in terms of the magnitude of removed risk and the costs of its implementation. A comparative analysis informs the decision-maker of risk reduction measures with similar attributes.

7.2.2 Application of the decision support methodology for cost effective selection of risk reduction measures

The significant advantage of the proposed approach to the existing cost-benefit approach in selecting risk-reduction measures is clarified by the following simple example. Suppose that a budget of £3 million has been allocated for the reduction of platform train accidents i.e. reduction in accidents involving passengers and trains at the platform area. This is a major risk which is located in the high-risk region of the risk matrix. The first risk reduction option 'A' requires the driver to operate CCTV monitoring of the platform. The train will not be started if there are passengers stuck at the door, fallen onto the track or fallen between the train and platform. Option B includes stop plungers - wall mounted alarm devices at specified locations/intervals within the platform area - which can be operated by platform staff or passengers. Trains in the platform area will be brought to a halt by operating any of these plungers. Option C consists of gap fillers between the train and platform to reduce accidents where passengers fall into this area when boarding. The three key risk reduction options, A, B and C have been evaluated, and the corresponding magnitude of removed risk and costs are shown in Table 22.

Table 22: Risk reduction measures with the associated costs and removed risks.

Risk Reduction Measure	Removed Risk [in millions £]	Cost of measure [in millions £]	Benefit/Cost ratio
A (One person operated CCTV)	2.0	1.60	1.25
B (Platform/passenger emergency stop plungers)	1.5	1.57	0.95
C (Gap Fillers)	1.2	1.3	0.92

To remove the major risk of a 'platform train accident' from the high-risk region of the risk matrix, the risk of minimum magnitude £2.5 million must also be removed. If the cost-benefit approach is used, the first measure, A, with benefit-to-cost ratio greater than one, will be the only selected measure. Measures B and C will be ignored because their benefit-to-cost ratios are less than one. The magnitude of the removed risk within the specified budget is £2 million – insufficient to remove the major risk from the high-risk region of the risk matrix. In addition, the magnitude of the removed risk could be significantly larger, considering the specified budget of £3 million. According to the proposed new approach, options A and C should be selected, because this is the combination whose cost is still in the allocated budget of £3 million and the magnitude of the total removed risk is the largest. Furthermore, the magnitude of removed risk according to the proposed approach will be £3.2 million, 60% more than the amount of risk removed by using the cost-benefit approach. As a result, the amount of removed risk is sufficient to remove the 'platform train accident' from the high-risk region of the risk matrix.

By applying the decision support methodology with the fundamental, verifiable risk reduction principles presented in Figure 52, the example of the real-life case in Section 4.3.3 can effectively be eliminated. In this particular case, the use of the key risk reduction principles with the proposed systematic and iterative process would have identified the inherent flaws from the application of axle counters, thereby significantly reducing overall costs. The challenges of the axle counter application are also a clear demonstration of the existing gap between the infrastructure and maintenance or operations within the railway organisation.

7.3 Evaluation of risk reduction implementation challenges in a railway organisation

The gap between the selection of risk-reduction options and the task of their effective implementation results in compromised safety and substantial losses. An effective risk management system must necessarily integrate the evaluation phases with the implementation phase of a project.

In a bid to continuously enhance safety and operational performance, the railway industry in the UK has invested several billions of pounds sterling into risk reduction and organisational structures. However, the best examples of risk management challenges and successes are relatively better published for other large-scale engineering projects as shown in the evaluations below.

As established by Van Der Merwe (2002a), hardly any publications exist on the effect that strategy, structure, processes and projects have on one another. He argues that an integration of *strategy, structure, processes and projects* is required to facilitate the effective development of a business. In an earlier work, Van Der Merwe (2002b) points to the *integration of organisational structure, control and prioritisation* as three critical areas necessary for effective risk reduction within large and complex engineering projects.

The key relationship between design, implementation and operational losses has been addressed in Hobbs and Andersen (2001), Neil and Fenton (2005) and Williams et al. (1995). Busby (1998) finds that feedback to designers is often unreliable, delayed, negative and sometimes non-existent. The study further shows that designers failed to learn from the feedback available, leading to development of plans that are at odds with past outcomes and repeat previous errors.

Millera and Lessard (2001) define risk on large engineering projects as the possibility that events, their resulting impact and *dynamic interaction* may turn out differently from what was expected. The risk of not completing the project is subdivided into technical*, construction and operational* risks. A study on how design errors can severely jeopardise safety and contribute to failures in construction and engineering projects, with devastating economic, environmental and social consequences, is presented

by Love et al. (2011). In this article, design errors are described as a symptom of dysfunctional organisational and managerial practices. Holzmann and Spiegler (2011) state that comprehensive product description and product requirements exert essential influences on the risk patterns of IT organisations.

By comparing product architecture to organisational structure, Gokpinar et al. (2010) describe the failures in large-scale product development processes as a misalignment of the organisation to the product. The authors point to two fundamental challenges: (i) the assignment of people to parts and subsystems that make up the product and (ii) the effective collaboration in the performance of design tasks. This is further supported by studies on railway organisational failures, primarily as a result of the misalignment between architectural/technical interdependence and organisational communication. Hansen (2002); Carlile (2002); Contractor and Monge (2002); Nonaka and Takeuchi (1995).

The risk of failure of large projects is a direct function of the level of interdependency among numerous parameters such as time, cost, scope, safety, environment, security and health. Within a project, the existence of interrelated risks naturally results in triggering one risk from another risk and creating propagation phenomena such as reaction chains, amplification chains and loops. Using a network theory-based analysis, Fang et al. (2012) proposed a risk reduction technique for failure within large projects. The paper also states that the risk of failure is caused *by the lack of capacity to anticipate and control complex interactions*. Corbett et al. (2002); Schlindwein and Ison (2004) and Baccarini (1996) share the same view. However, Vidal et al. (2011) goes further by proposing that the key factors that drive complexity are project *size, variety, interdependence and context*.

The underpinning requirement for an effective organisation is that the latter must successfully assimilate and implement technology, and manage interactions between the source and the recipient of technology. *The capacity to efficiently act on knowledge is argued to be a critical activity that determines the readiness and value of an organisation's structure* (Wong et al. 1998). To build on this point, it is important to note that any effort towards risk reduction must comprehensively consider the source of risk and the receiver, before any claims for effective risk reduction can be made. According to Ahonena and Savoleinena (2010), the primary causes of failure for major engineering projects are: *the lack of understanding of users' and operational needs, poor staffing decisions, tight schedules and extensions to the functionality of an existing product without a comprehensive understanding of the technical challenges.*

The studies on the effectiveness of technology innovation, implementation and risk reduction have accumulated and advanced over a number of decades. The partitioning and interdependency of risks associated with the conceptualisation and execution phase are best presented by McFarlan (1992).

Innovation is partitioned into an initiation phase and an implementation phase, as shown in Zaltman et al. (1973). Within an organisation, high complexity, high diversity, low formalisation and low centralisation are most conducive during the initiation phase, whilst low complexity, low diversity, high formalisation and high centralisation are most conducive at the implementation stage. In line with this theory, Baker and Sweeney (1978) demonstrate the potential constraints arising from inadequate specific knowledge of the project and the mutual self-reinforcing relationship between organisational structure and project. A later study by Remenyi and Heafield (1996) also pointed out that organisational structure, corporate culture and people are primary risks.

The risk of failure during implementation is three-dimensional in project size, experience with the technology and organisational structure. Willcocks and Margetts (1991), Bessant (1991) cite amongst other factors, the lack of organisational adaptation to complement technological change. An example of inappropriate applications is the introduction of new trains in small tunnels when it would have been easier to introduce advanced vehicle controllers only, at lower cost. Other important factors contributing to the risk of failure are the lack of skills to support implementation and the lack of exploration of a wide range of options.

These studies clearly demonstrate that the organisational structure is impacted by the risk reduction options selected and *vice versa*. Consequently, for effective risk reduction, it is mandatory to establish the relationship between risk reduction at the initiation stage (i.e. the stage of identifying and assessing risk reduction options) and risk reduction at the implementation (operational) stage, where there is a significant contribution from the organisation and users. Figure 53 illustrates the weaknesses in the implementation phase that could partially or fully compromise the high level of potential risk reduction achieved at the initiation stage. In order to achieve and maintain a maximum risk reduction, the organisation *must demonstrate readiness for acceptance and effective implementation of the risk reduction options identified at the initiation phase. These may include new techniques, technologies, processes etc*.

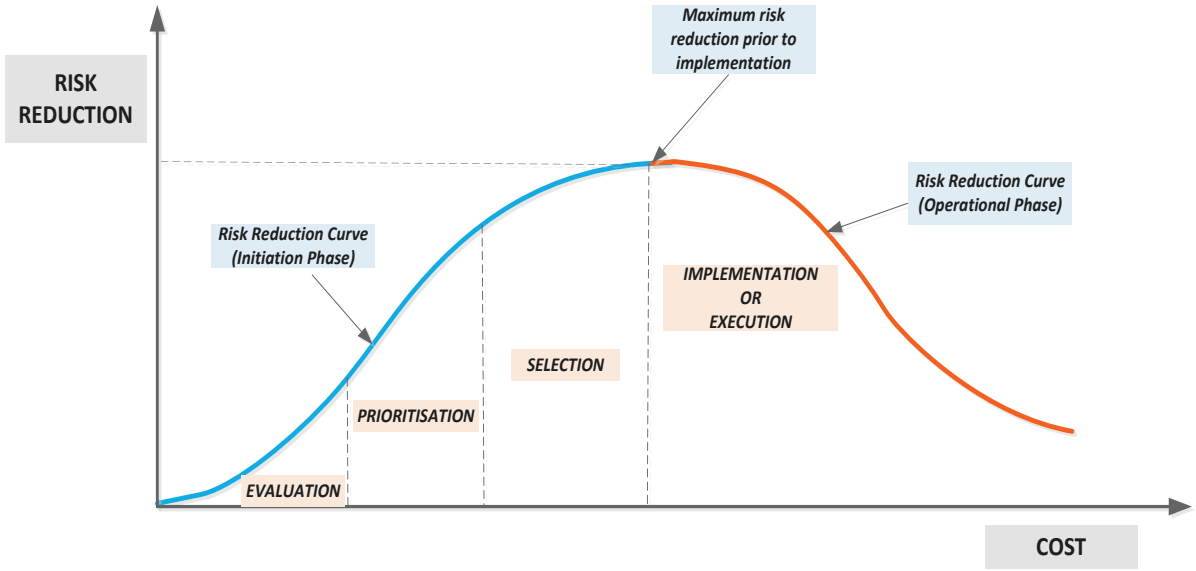


Figure 53: A Risk Reduction Curve due to a poor implementation of the risk-reduction options selected at the initiation stage

During the initiation or concept phase, the risk reduction evaluation effort is controlled by a complete and well-defined set of safety requirements. During the implementation phase, the integration of several options has the potential to expose an organisation to unanticipated problems and vulnerabilities. The novelty of the risk reduction measures plays a major role in the implementation stage. At the initiation stage, the scope of integration activities to be performed for novel measures must be identified and well defined with all potential integration risks assessed and prioritised. In effect, introducing risk reduction measures without proving their integration at the earliest possible opportunity means that the overall risk reduction objective can be defeated.

These problems are further compounded by an inefficient organisation. The specification of requirements must identify potential stakeholders. This ensures that the proposed solution is not only cost effective (i.e. feasible and affordable), but also guarantees the required levels of risk reduction. Most system engineering applications use system context diagrams and system architecture to identify all interfaces and provide an overview of the interface risks. Each interface can then be assigned an owner who will be the stakeholder at the interface. This individual will have the technical authority to influence progress and manage risks relating to the interface up to closure.

On a large and complex project, the primary requirement for maximum risk reduction within a fixed budget is that the selection of risk reduction measures complies with the risk reduction potential and the budget constraints. This also requires a methodology that facilitates a comprehensive evaluation of the selected options. All operating modes (normal, degraded and abnormal) and the transitions between them should be considered. The way in which the systems will be operated, including the capacity and

competence of personnel involved, operational arrangements and processes need to be fully understood in order to address the full set of possible operational scenarios. The integrated systems in the risk reduction exercise are a complex combination of people, processes and supporting structures (i.e. equipment or tools), whose interaction must be fully understood in order to achieve efficient risk reduction.

7.3.1 Inter-relationship between risk reduction evaluation and implementation

The introduction of new techniques, technologies or processes into the railways is usually associated with complexity and uncertainty. Whitty and Maylor (2009) qualify projects as *dynamically* or *structurally* complex and broadly dependent on project elements and interactions that are subject to change. This results in unpredictability, uncertainty and emergent behaviours. Structural complexities, on the other hand, are quantifiable and predictable, which provides an opportunity for better management. Koppenjana et al. (2011) provide insight into the complexities and uncertainties involved in the risk reduction and effective management of large railway projects, in cases where there is predictability and in-built flexibility in the organisational structure.

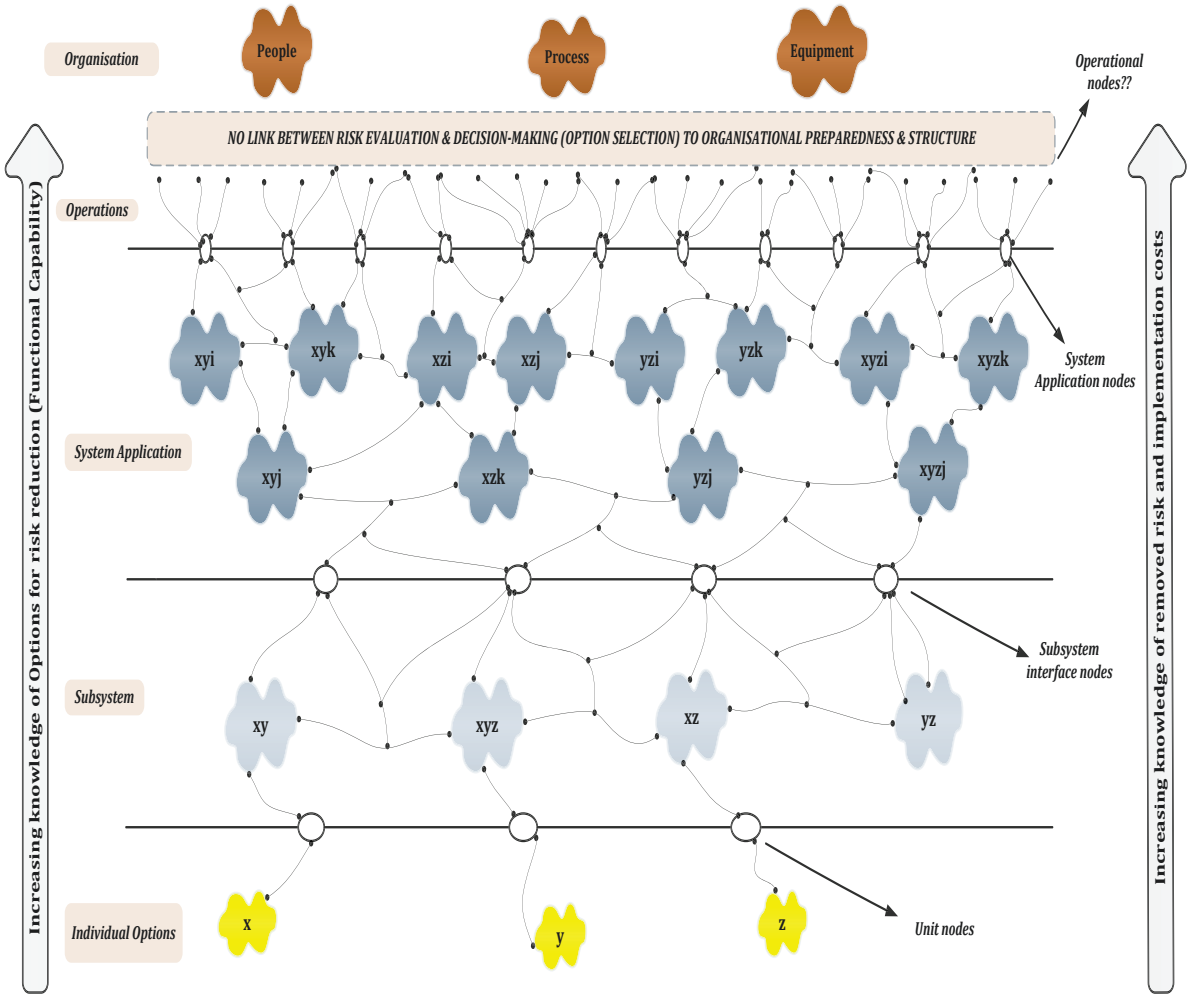


Figure 54: A system analysis is necessary for the effective implementation of the selected risk reduction options.

Figure 54 provides a simple illustration of the interactions and dependencies between risk reduction measures and the application environment, which includes people, processes and equipment necessary for effective implementation. This figure raises a fundamental question – is the railway organisation adequately built to facilitate the implementation of the selected risk-reduction options? **In the current system, there is no link between the evaluation phase and the implementation phase of risk-reduction**.

A simple practical illustration is the application of a number of risk reduction options to reduce the *Collision Between Trains* accident. The options are generally classed as (A) *brake assist systems*; (B) *collision warning systems* and (C) *intelligent speed adaptation systems*. These three options achieve the risk reduction because of their inherent operational characteristics. In practice, these options are not mutually exclusive and an investment in all options (A, B and C) is often required to achieve effective risk reduction. While for risk reduction options which are relatively independent, the application of dynamic programming techniques is fully justifiable and leads to a significant risk reduction within a fixed budget

Todinov and Weli (2013), additional (systems) analysis is needed for correlated risk reduction options. In cases where some of the options are incompatible (i.e., cannot be applied simultaneously) or in cases where the effective risk reduction from the application of one option requires the application of another option, the blind application of mathematical optimisation tools may not result in the expected risk reduction.

The limitations, the required conditions, and existing interactions among the risk-reduction options should be thoroughly understood and accurately specified.

Additional risk reduction options, typically introduced in railway safety to reduce the Collision Between Trains accidents include: extension of signals, train movement rules, incident response systems, train driver training, speed restrictions, wheel-slide protection systems, In-cab design modifications, operational testing and maintenance, emergency timetables, track inspections and refurbishment, one-person (driver) operated closed circuit television, etc.

Consequently, a number of additional measures can be combined with the selected options A, B and C to achieve a significant risk reduction:

Option A: Brake assist system + (operational testing and maintenance, train driver training, one person-operated closed circuit television)

Option B: Collision warning systems + (train driver training, in-cab design modifications, speed restrictions, emergency timetables)

Option C: Intelligent speed adaptation + (Train movement rules, wheel-slide protection, extension of signals, emergency timetables)

For example, investing in brake assist systems (Option A) without investing in operational testing and maintenance does not permit a long term risk-reduction benefit from investing in expensive brake assist systems. Option A also requires investment in testing and maintenance if a long-term risk-reduction effect is to be achieved. Similarly, investing solely in collision warning systems (Option B) without simultaneously investing in driver education and training does not result in a tangible risk reduction benefit from applying solely Option B. As a result, if Option B is to have a tangible risk-reduction effect, investment in another risk reduction option (‘driver training and education’) is necessary. In fact, without driver training and education, there may not be any risk reduction benefit from the purchase of expensive collision warning systems.

7.3.2 Risk Reduction Readiness Model

There is surprisingly little research on the risks involved in the implementation of risk-reduction measures within the railway organisation. Current studies, mostly of organisations' internal risk management practices are limited in scope and cannot be generalised. In addition, there are no standard measures of effectiveness for the implementation of risk reduction options, until an accident occurs. Most ALARP or risk management studies have been limited to identification, evaluation and options selection without any supporting analysis on the applicability of the selected options within the railway organisation. Any knowledge in this area is hardly ever recorded and definitely not incorporated in existing safety and business cases, despite the potentially severe financial and safety consequences. The existing safety and business cases do not analyse the risk reduction measures in relation to their mutual correlation, suitability and implications for the organisation. Without an organisational readiness to support effective implementation of the selected risk-reduction options, the existing safety and business cases are inadequate and weak.

The major determinants of cost, schedule and risk reduction is the people-process-systems triad discussed in the system engineering approach (Section 7.1). Out of these, process is often considered the glue that keeps the triad together. Interestingly, Lockamy and McCormack (2004) use the concept of process maturity (which assumes that progress towards a goal comes in stages) to examine the relationship between supply chain management process maturity and performance. The paper further suggests a supply chain management process 'maturity model' for enhanced performance in this area. The concept proposes that a process has a lifecycle that is assessed by the extent to which the process is explicitly defined, managed, measured and controlled. The concept also implies growth in the areas of process capability, richness and consistency across the entire organisation.

Within an organisation that controls risks, ambiguous specifications and requirements for risk reduction, lack of clarity on the inter-relationships between risks, risk reduction options and the associated functions are major negative factors. The issues related to managing multiple projects such as prioritisation, selection and resource allocation in multi-functional organisations, are well defined in Patanakul and Milosevic (2009); Seider (2006); Hendriks et al. (1999); Nobeoka and Cusumano (1995). These issues are very similar to managing and implementing multiple risk reduction measures.

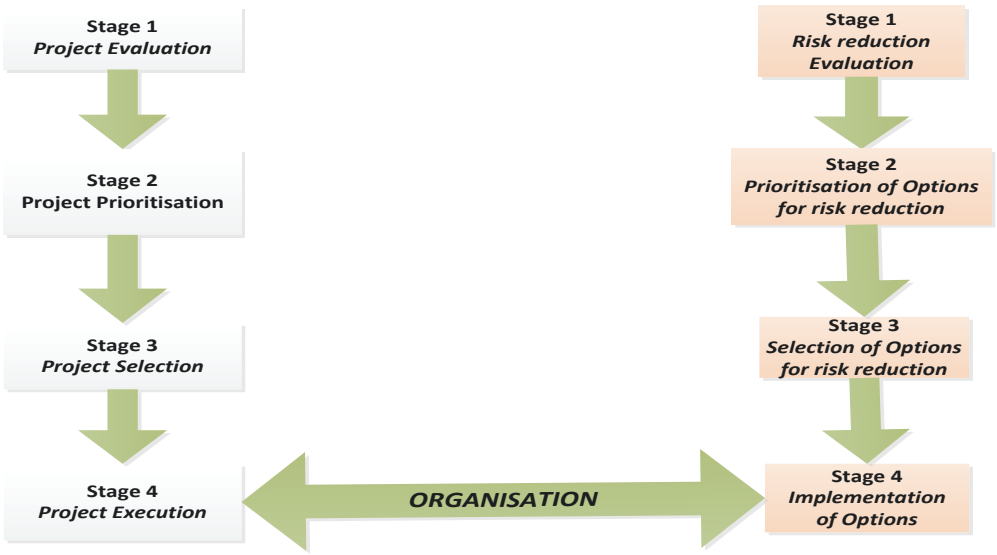


Figure 55: Parallelism between the implementation of multi-functional projects and the implementation of risk reduction measures.

The left-hand side of **Figure 55** illustrates the key stages of effective management of projects. The essential stages in the implementation of risk reduction measures are provided in parallel (the right-hand side of the figure). The diagram clearly illustrates an existing parallelism. The benefit of an improved organisational readiness has another, very important dimension: the capability to address unanticipated risks. These circumstances cannot be predicted, and are 'unknown unknowns' or 'black swans' (Taleb, 2007). However, we do know they might occur. Improving the risk knowledge, the safety culture in the organisation, and the level of general risk protection measures are effective barriers to unknown unknowns.

A change in the organisation structure may be necessary to effectively implement particular risk reduction options. This is the case when considering two options to eliminate wrong-side failures (i.e. failures leading to catastrophic consequences) for spring-applied parking brakes by either

- Enhancing testing and maintenance regimes or
- Replacement with new braking systems.

Selecting and implementing enhancing testing and maintenance regimes, for example, requires specific organisation changes, (such as developing an organisation with emphasis on maintenance and testing rather than one with key expertise in design and manufacturing) for maximising risk reduction. These organisational changes are driven not only by cost considerations. More importantly, they are the only way to guarantee that effective risk reduction will be maintained through the life of the operation. In common industry practice for selection of risk-reduction

options, no publication, significant work or structured guide exists beyond the standard risk evaluation methods based on cost-benefit analysis (CBA). In fact, the existing approach does not consider the organisational structure (people, processes and tools/equipment) and its preparedness for the selection, evaluation and implementation of the risk reduction measures. The consequences of this lack of appropriate structure are:

- Incorrect evaluation of risk-reduction options, resulting in:
  - Reduced safety levels
  - Increased implementation costs
  - Inaccurate prioritisation of the risk reduction measures
  - Incorrect estimation of residual risks
  - Inaccurate risk profile
- Misalignment of selected risk-reduction options with the organisational capability and management structure, which leads to
  - Increased risk of failure to gain approval for the selected risk-reduction measures
  - Increased implementation costs
  - Inadequate implementation leading to degraded safety levels

Considering these consequences and existing practices, four distinct levels of readiness for implementing risk reduction have been identified for railway organisations. Table 23 presents the Risk-reduction readiness levels for railway organisations.

Table 23: Classification of railway organisations - level of risk-reduction readiness

Risk Reduction Readiness Levels	Strategy	Description
Level – 1	Reactive level	No risk reduction strategy. Reactive approach to risk management (dealing with risks as they materialise)
Level – 2	Basic level	Basic risk reduction based only on qualitative assessment and measures (e.g. by using risk matrix)
Level – 3	Normative level	Risk reduction based on cost-benefit analysis, which involves quantification of risk reduction options in terms of benefit and cost). No methodology for selecting risk-reduction options. No consideration of the interaction among risk reduction options. No optimisation in selecting the risk reduction options. No consideration of the impact of the selected options on the organisation and the environment. No consideration of the required organisational changes needed for the implementation of the selected options.
Level – 4	Optimal level	Risk reduction is based on a systematic approach impacting the risk option selection, the precise quantification of removed risk and the optimal selection of risk reduction options. The impact of the selected options on the organisation and the environment is part of the analysis. The required organisational changes needed for the implementation of the selected options are carefully considered and specified.

Organisations at Levels 1 to 3 do not provide any support for maximising risk reduction within fixed budgets. This increases an organisation's vulnerability to inaccurate assessments of risk and selecting weak and inefficient risk reduction options at escalating costs. The proposed classification, based on fundamental principles of risk reduction and systems engineering is an initiative with the potential to provide a Level-4 framework that supports risk evaluation, optimal options selection and ultimately permits organisations to maximise risk reduction within fixed budgets. The proposed classification also bridges the gap between evaluation and selection of risk reduction options and specifying adequate organisational structure for their effective implementation.

7.4 A new classification of risk reduction options

As established, integrating risk evaluation with primary operational functions is a fundamental requirement for successfully making the case for the selected options. This requirement is especially valid to industries where risk management drives investment and decisions. Bessis (2002) and ROGS expound on the topic related to effective management of operational risks. These risks are defined as event risks and to effectively handle the risks of potential losses, categorisation of events is necessary. This serves as a receptacle for accident data gathering on frequencies and costs. A tentative categorisation for managing potential operational losses is further provided as People, Processes, and Systems.

The Railways and Other Guided Transport Systems (Safety) Regulations requires that the infrastructure operator and maintainer of the railways demonstrate how safety risks will effectively be managed and whether the infrastructure operator and maintainer have the ability, commitment and resources to comply with the regulations. This is generally addressed by:

- *Demonstrating capability, commitment and availability of resources to manage safety risks;*
- *The safety case which provides a framework against which regular assessments, risk control measures and management systems are established and maintained;*

The safety case assures regulators that the risks associated with operations have been assessed and all reasonably practicable controls have been implemented to reduce the risks.

The areas that are considered safety-critical and have a direct impact on the successful prevention of accidents on the railways are typically *signalling and train control (communication systems); train driving and train operations; train manufacture, maintenance and refurbishment; installation, renewal and maintenance, faulting and inspection of infrastructure; safety of passengers on trains; passenger and visitor movement on stations and platforms; on-track machine manufacture, maintenance and*

refurbishment. The major risks that are to be reduced are the *risk of derailment*, *risk of collision between trains* and *risks related to the passenger train interface*.

Following the argument that effective risk management must integrate the two phases of initiation (evaluation) and implementation, a categorisation of risk reduction measures that best addresses a standard railway industry portfolio is introduced. The introduction of a structured approach based on categorising the options for reducing major accidents, reflects the standard railway organisational structure. By categorising these options into *design, operational, procedural and technical options*, it is guaranteed that the efforts of the implementation facilitators (people, processes and supporting systems) are systematically harmonised. The categorisation effectively simplifies a complex register of risk reduction options and combination of options into a format that reflects the typical railway organisational structure and helps reduce the gap between the evaluation and implementation phases.

The categorisation includes:

- *Design risk-reduction options (DRRO)* – Novel systems, major renewals and modifications
- *Operational risk-reduction options (ORRO)* – Communications, Supervision and Speed Restrictions or similar operational decisions
- *Technical risk-reduction options (TRRO)* – Testing, Maintenance, Inspections, Installations, Assessments/Studies informing risk reduction decisions
- *Procedural risk-reduction options (PRRO)* – Risk education, Risk training, Processes and Plans

Each risk reduction option, within each group, is based on sound engineering principles for risk reduction. Theoretical considerations, reliability, risk modelling, field-testing and historical track records have proved the effectiveness of each of these options. The introduction of these options reduces the complexity of selecting risk reduction options for different applications. At the same time, the classification guarantees that no efficient risk-reduction option is missed at the evaluation phase. Consequently, this classification will be particularly useful for major railway projects with numerous possible risk reduction options, typically reflecting all aspects of the standard railway organisational operations including: *design*, *maintenance*, *testing, new technologies* etc. *combined with people*, *processes and equipment*. Table 24 presents a structured categorisation that supports the option selection and the evaluation of individual options or combination of options. The systematic process of categorising the risk reduction options and aligning them with the existing organisational functions also supports the identification and assignment of responsibilities for effective implementation. Table 24 and Figure 56 also illustrate the relationship between the major accident hazards, risk reduction measures and the direct link with the organisational instruments – people, process and equipment. Figure 56 also depicts the role of the proposed categorisation for effective risk reduction.

Table 24: Categorisation of risk-reduction options in the railway industry.

RISK REDUCTION OPTIONS	EXAMPLES OF RISK REDUCTION OPTIONS	Key Function(s) for implementation
DESIGN OPTIONS (DRRO) **Novel Systems, Major Renewals, Design Modifications (Capital Intensive Projects)**	1. Signalling replacements and modifications - automatic signalling and control systems 2. Optimising cab design for driver protection	Chief Engineer, System Integration, Programme Directorate, Project Management
TECHNICAL OPTIONS (TRRO) **Testing, Maintenance, Inspections, Installations, Assessments/Studies**	1. Improving inspection, testing and maintenance regime for detection of wheel flat and worn wheels 2. Signal positioning studies and potential extension of distances between signals	Technical Assurance, Civil and Power Engineering, Signalling Systems Engineering, Train Systems Engineering, Asset Management
PROCEDURAL OPTIONS (PRRO) **Risk education and training, Processes and Plans.**	1. Risk education and training of key personnel 2. Amendments to train despatch rules 3. Review and improvement of recruitment and selection processes	Infrastructure and Systems Protection, Training Management or Organisational Development.
OPERATIONAL OPTIONS (ORRO) **Communications, Supervision and Speed restrictions**	1. Crowd Control 2. Speed restrictions (adhesion)	Operational Engineering, Telecommunications Systems Engineering

The clear outline of the roles and responsibilities within the risk reduction exercise ensures that resources such as finances, technical expertise, information, systems and equipment, medical facilities etc., necessary for implementing the measures are available and appropriately targeted. In the risk reduction effort, undertaking emergency and preparedness planning, immediate post-accident actions and response is absolutely essential. The inter-relationships between departments participating in the risk reduction operation can be used for developing measured strategies for accident prevention and protection. Throughout the project lifecycle, the clearly defined inter-relationships between departments ensure that the railway operations also make it possible to take advantage of the many technical resources that already exist within the organisation.

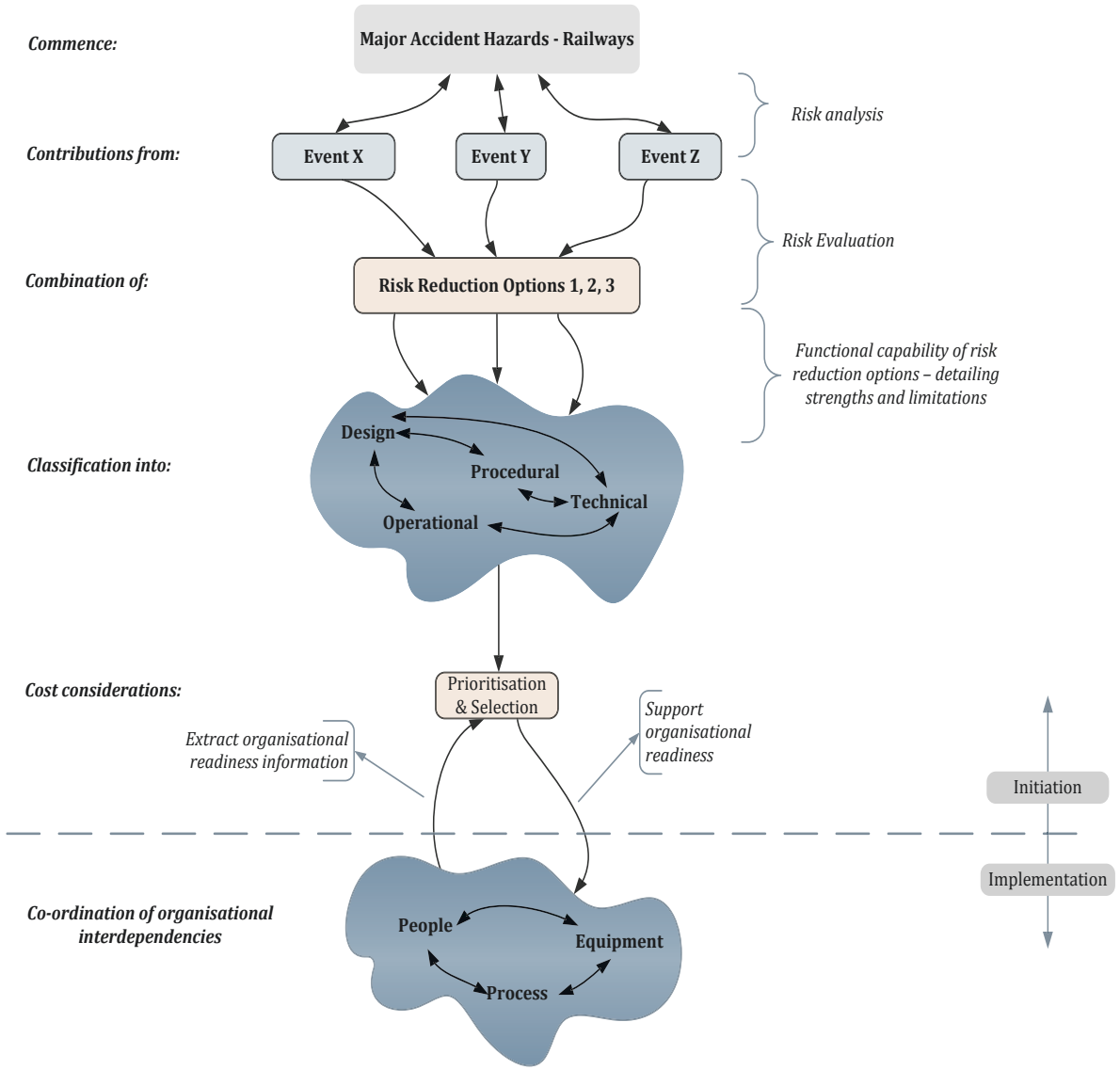


Figure 56: Categorisation of risk-reduction options, risk management and the organisation

The proposed classification promotes a comprehensive understanding of the risks resulting in an accident and provides a strong support to the *Lessons learned database*. It provides a direct and strong support to the comprehensive check lists related to known accident scenarios which is an important tool for identifying possible accident and failure scenarios. The proposed methodology also draws on concepts from organisational theory and optimisation of risk reduction as introduced by Weli and Todinov (2013). However, by considering the intricate interrelations between risk reduction options and the organisational interdependences, it goes beyond the development in Weli and Todinov's paper and promotes a novel framework that bridges the divide between the identification and implementation of risk reduction measures within railway organisations.

7.4.1 Readiness for effective risk reduction

A significant amount of effort towards risk reduction in the railway industry is associated with major renewal projects. The renewal projects are usually large-scale engineering undertakings that provide the railways with necessary modifications and improvements. Along with reducing particular risks, these projects introduce new risks to railway operations. Consequently, essential risk reduction measures are considered and implemented to ensure that the safety integrity of the railways is not compromised, and where possible, improved. The new risks result from altering fundamental operational parameters such as *increasing number of trains to cater for a greater passenger volume* or *the removal of speed limits to meet operational schedules*. The situation is complicated considering that these changes are weather-dependent – they are different during different times of the year. The challenges facing the railway industry are the unrelenting pressures to reduce cost, improvements for customers and pressure to maximise the use of the asset base.

However, the organisational changes and modifications, every time a big renovation project is initiated, are very costly. A railway organisation that has not taken the necessary steps to a dynamic and flexible organisation in relation to risk reduction, easily incurs significant implementation costs. The significant increase in implementation costs usually deters the selection of appropriate risk reduction options to achieve a maximum risk reduction.

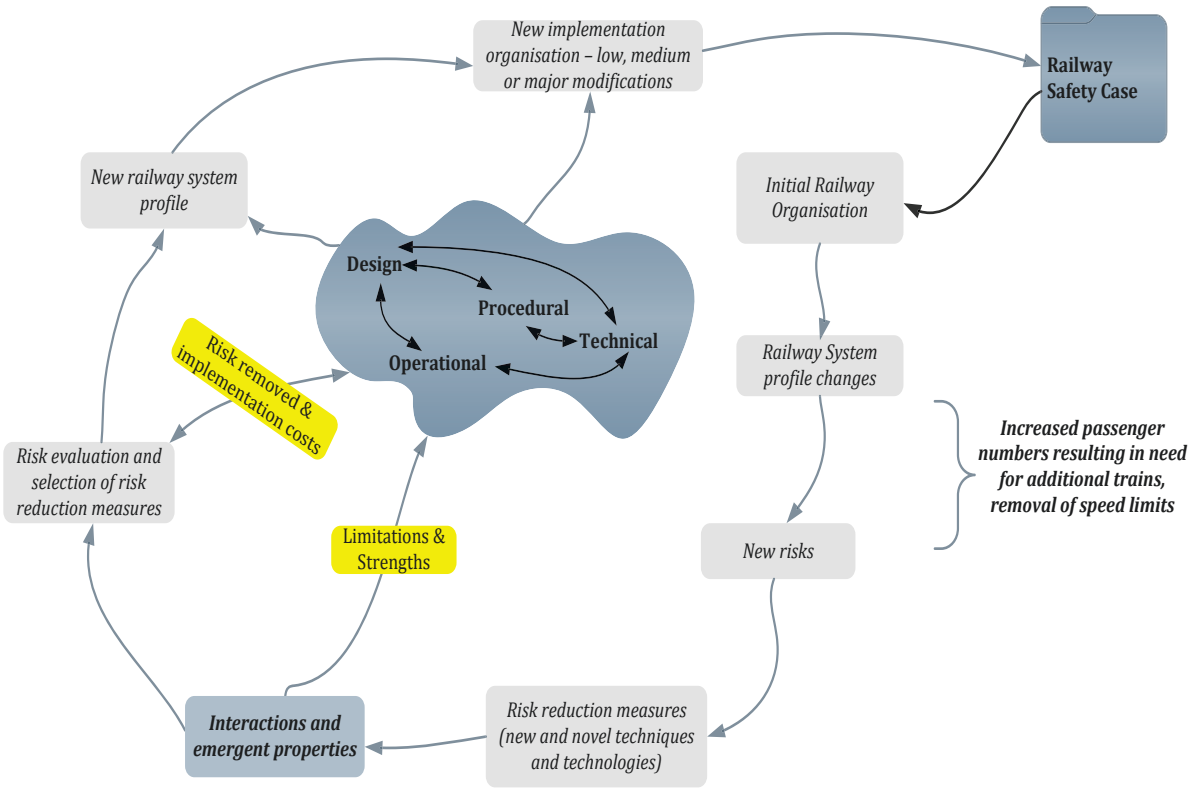


Figure 57: **New operational modifications and the process of risk reduction associated with the new risks.**

By adopting the proposed categorisation technique, the organisation is less likely to invest in new organisational development and re-structuring schemes that facilitate the required modifications.

The comprehensive decision-support framework provided by the proposed categorisation strengthens the assurance case for organisational readiness prior to gaining approval to operate. Essentially, it is recommended that to achieve a maximum risk reduction within financial constraints, the concept of *'Readiness for effective risk reduction'* be stipulated as a fundamental process requirement in railway safety cases.

It is essential that modifications and potential changes to the operating parameters leading to modifications are properly assessed and not imposing fundamental changes on an existing railway organisation. Without the structure proposed, any rapid evolution of the railway organisation will certainly result in excessive implementation costs. By improving an organisation's readiness to implement effective risk reduction, significant cost savings and improved safety levels can be secured.

7.4.2 The DOPT Assurance Case

The existing safety and business cases that support project acceptance provide insufficient guarantees that the organisation is ready and capable of undertaking massive safety-related projects. Conversely the Design-Operational-Procedural-Technical (DOPT) methodology provides the decision maker with a structured, simplified and easily understood technique.

DOPT classification is derived from basic principles of risk reduction and systems engineering to address the existing gap between the initiation (evaluation) phase of risk reduction options and the implementation phase. The DOPT methodology creates a common categorisation of risk reduction measures that best addresses a standard railway industry portfolio.

The DOPT methodology requires a thorough understanding of the budget location methodology. This means that as a minimum, the capability of the measure to reduce the likelihood of the accident or its consequences must be thoroughly understood. The DOPT concept permits effective planning of human resources, spheres of responsibilities and equipment engaged, taking into account the capabilities of the railway organisation. The clear outline of the roles and responsibilities in the context of risk reduction ensures that resources such as finance, technical expertise, information, systems and equipment, medical facilities etc., required for implementing the measures are available and appropriately targeted.

A framework for reducing the duplication of effort is provided using DOPT as it supports further considerations of whether the organisation or specific departments within the organisation are better placed to implement the risk reduction measure or combination of measures for any particular risk. The technique also creates a common risk-reduction platform between departments to ensure synergy in the risk-reduction effort. It supports technical co-operation for the effective use of preventive and protective risk reduction measures. It establishes and implements robust accident prevention programmes and mitigates against the consequences of an accident.

Most importantly, the Level-4 Risk Reduction Readiness that supports risk evaluation and optimal options selection permits organisations to maximise risk reduction within a fixed budget. The use of a methodology similar to the proposed DOPT methodology is a hallmark of an organisation possessing a superior level of risk-reduction readiness.

7.5 Risk reduction (safety) in contracts / procurement

All projects have an element of risk within the contract from which they have been set up. From the initiation stage of a project, establishing a proactive risk management system significantly increases the likelihood of meeting the overall risk reduction objectives. In general, for progressive risk reduction at all levels of an organisation, technical co-ordination or management is a fundamental requirement.

A management framework that includes techniques for insuring contracts assures competency within the supply chain, and reduces the safety risks introduced by contracts. The detrimental effect of the unknown risks and more specifically, the difficulty in predicting the extent of risks introduced by contracts necessitates substantial compensations for long-term projects. This translates into an accumulation of risk premiums throughout the project supply chain. The exponential growth in such premiums further translates into higher charges for the services provided. The growth in risk premiums reflects the inability to manage risks rather than a more efficient transfer of risk responsibilities (Ng and Loosemore, 2007). Wagner and Bode (2007) agree that the supply chain risks are also triggered by a series of catastrophic events that have disrupted economies and supply chains around the globe. These events, including numerous examples from the railway industry, increase the need for emphasis on the vulnerability of contracts and supply chains.

Descriptive examples of major UK railway projects that have faced considerable criticism due to failure of contracts are well documented. Through a brief evaluation, this work confirms the vital role played by contracts in risk reduction measures selection and implementation. Most importantly, they propose a simplified approach to elimination, and where this cannot be achieved, at least to reduction of the impact from incorrectly specified contracts.

7.5.1 UK Railway Contracts – Public Private Partnerships

Due to the capital-intensive requirements of undertaking major railway projects such as the London Underground renewal projects, the Sydney Metro project, Beijing Metro and similar projects in Hong Kong, Singapore, China and the USA, there is an increasing move towards shared public/government and private financing initiatives.

Most major UK railway contracts are in one form or another of public private partnerships (PPP). The majority of railway failures or accidents during a PPP project period are quite easily labelled ‘contractual’. This suggests that the flaws in these PPP contracts are generally perceived by the customer as the root cause, and requires a change in the existing frameworks. In the case of the UK railways, the customers are the passenger and tax payers. Examples of these contract debacles are those of the London Underground PPP, the West Coast Main Line project, and the operational railway contracts debacle that recently generated significant issues between two major train operators and the Department for Transport (DfT). The potential effects on safety risks as a result of the PPP contracts were furiously debated by the House of Commons (2002) and are of great concern to the public and taxpayer. However, evidence that the PPP contracts negatively impacted railway safety is not as widely documented.

The PPP, an evolving concept, is essentially an arrangement by which private parties participate in, or provide support for the provision of infrastructure-based services. PPPs are not a typical public

procurement, which involves the public sector purchasing an asset. Rather, a PPP system involves the purchase of a stream of services, defined in a detailed service agreement. (Ng and Loosemore, 2007) classify risks in PPP projects into two main groups: general risks or project risks and affirms that special risks associated with PPP procurement process are to be considered. Structured arguments against PPP with regards to contracts and procurement are presented in Jones (2002); Moore and Muller (1989); Grimsey and Lewis (2004). These criticisms relate to the significant risks retained by the procurer; and exorbitant risk-related service charges for the public. These contracts are not economically viable; they introduce a greater degree of waste and rework as a result of complex and long tendering, and excessive post-tendering negotiation. The last two issues are caused by the additional need to satisfy several stakeholders, and the complexity of contracts.

Jean Shaoul (2002) analyses the implications of the LU PPP cost structure and evaluates the methodology for appraising the PPP. She finds that the methodology cannot be relied on to provide sound decision-making tool for London Underground, as the risk reduction methodology does not account for additional risks introduced by PPP. In concluding the evaluation, the paper states that the main risks are those that arise from technical obsolescence, changing regulation and demand. The paper also identifies important factors, albeit not directly safety-related but noteworthy, to illustrate the weaknesses in one of the most publicised UK railway PPP contracts. The obvious weaknesses in the contract that resonates in the current economic state include:

- No consideration of the impact of any recession during the 15-year period on passenger numbers. This has proved to be detrimental to the implementation of the contracts.
- Assumption that the cost of operating passenger services will decline, even though the new organisational structure has resulted in additional costs.

Considering that primary public objective of any contract is ‘Value for Money’, while a primary private objective is profit maximisation, Gordon et al. (2013a) raise the question ‘How can the interests and objectives of contractual partners be aligned in the contract?’ Gordon et al. (2013b) further propose that the solution to this lies in appropriate incentives and results in ‘optimal contracting’. The two explicit incentive elements presented are performance payments, penalties and appropriate risk allocation. The implicit incentives include performance targets met during tender or contracting process, design, contract term and the institutional structures or formations.

Following an evaluation of different literature on achieving effective risk allocation PPP contracts, Ke et al. (2010) present a comparative analysis of risk allocation preferences. For the scope of this work, the comprehensive list is reduced to directly illustrate the potential safety-related risk factors and allocation preferences in the PPP contracts evaluated (Table 25):

Table 25: Risk allocation preferences for safety-related contract risk factors

Risk factor	Risk Definition	Risk allocation
Availability of finance	Potential difficulties in financing the tasks	Private
Improper design	Neglect of inherent design safety principles	Private
Quality risk	The absence of demonstrable evidence that a basic quality management process has been followed may signify underlying risks – heavily weighted on unknowns	Private
Site safety	Responsibility for customers (or passengers) and workers (staff)	Private
Design changes	Unanticipated changes and errors in the design resulting from improper specifications	Public
Unproven engineering technologies	The technology adopted being immature or unable to meet requirements – including technology qualification risks	Private
Operator defaults	Operations cost overrun resulting from improper measurement, ill-planned schedules or low operation efficiency	Private
Frequency of maintenance	High level of intervention on systems affecting operations and potentially compromising system integrity	Private
Residual assets risk	Assets transferred to the asset owner at the end of the concession period normally have residual risks that must be addressed prior to handover	Private
Condition of facility	Unavailability of supporting facilities to achieve safety and performance requirements	Private
Weather	Poor or unexpected weather conditions resulting in rail/wheel interface risks or increased likeli-hood of failure/accident	Public
Changes in industrial codes of practice	Inconsistency in technical standards influencing the scope and function of the tasks	Shared
Project Approval and Permits	Delay or refusal of project approval and permit	Shared
Organisation and co-ordination	An increase of transaction cost or a dispute may occur because of improper organisation and coordination	Shared

In a thorough assessment of the well-publicised condemnation of the London Underground PPP contracts, Jupe (2009) argues that public transport PPPs require complex contracts underpinned by regulatory mechanisms in order to maintain performance and safety standards. Additionally, the paper insists that risk transfer is difficult to achieve, as essential infrastructure cannot be left to the ultimate market discipline of bankruptcy. Critiques from the House of Commons Select Committee on Transport identified serious concerns from implementation of the PPP contracts that could potentially compromise safety as:

1. The complexity of the management arrangements of the contracts
2. The conflicts with safe working practices as a result of the pressure to deliver required improvements under the contract performance regime
3. Shortage of funds constraining capacity improvements
4. Constraints on risk transfer
5. Impossibility of quantifying some key (subjective) factors in the assessment of value for money

Liu and Wilkinson (2013a) show that for a successful PPP contract the following key features must be considered:

1. Sound business case development
2. Streamlined financial agreements
3. Robust tendering
4. Effective governance and partnership-based consortium
5. Realistic risk allocation

Despite the criticisms of government and private partnerships or initiatives, Sarathy (2006) maintains that such partnerships are required to improve safety and security in the supply chain.

The concept of partnering underlines that mutual objectives between the parties should be agreed upon and regularly reviewed. Prior to the partnerships that blighted the railway industry, it was expected that the partnering concept would provide an opportunity for continuous improvement of overall risk reduction, including safety performance. Partnering was entertained and indeed adopted on major UK railway projects as it provided an ideal opportunity to move away from prescriptive- to performance-based legislation in the regulation and implementation of safety Matthews and Rowlinson (1999). A comprehensive study on the effectiveness of safety-based incentives in PPP contracts has been used to demonstrate that the implementation of safety incentives in PPPs has a positive influence in the reduction of fatalities, injuries and accidents (Rangel et al., 2012).

With this in mind, it is necessary to formulate a framework that will have a credible effect on understanding and improving deliberations and agreements on major railway contracts. The safety risks introduced by such partnerships should be well defined and subsequently assessed prior to contract awards or agreements. The approach of using basic engineering and management principles is illustrated as effective in the next section where different techniques are developed for managing the complexities of safety contracts resulting in product failures.

7.5.2 Supply Chain risk reduction – product safety and recalls

Immediate commercial and safety risks associated with an incorrectly specified contract agreement between a client and the contractor include integration risks, maintenance or intervention, increased product recalls and the risk of failure to gain approval as a result of design failure. In the specific area of managing risks associated with product recalls, Pyke and Tang (2010) use the continuous improvement process to support the 3-R approach. The 3-R approach uses three parameters: readiness, responsiveness and recovery for managing product safety and recalls. Kumar and Schmitz (2011) also present an active application of Six Sigma in the control of risks of product recalls. An intriguing article by Hora et al. (2011) provides a good analysis of the impact of the time to recall defective products, its impact on safety risk and the role of the supply chain in risk reduction. This paper strongly argues that the relationship between time to recall and effectiveness of the recalling organisation's supply chain depends on:

- The recall strategy (preventive vs. reactive) adopted by the firm;
- The type of product defect (manufacturing defect vs. design flaw);
- The supply chain entity that issues the recall

There has also been a steady increase in publications and research work in the area of product safety as it relates to supply chain risks. Notable works include Kleinforder and Saad (2005) whose interesting combination of supply chain agility, supply chain optimisation, supply chain information sharing, flexibility and modularity, total quality management (TQM) and contingency planning is effectively demonstrated as a good management approach. The use of TQM could be appreciated and justifiable if focus is primarily on the bottom-line. The neglect of product quality and safety is identified by Minhyung (2010) as the major reason for the substantial and widely publicised 2010 Toyota recalls. Other works by Tang (2006); Lee et al. (2008) are equally noteworthy. With a view to evaluating the effect of the global supply chain in creating or exacerbating safety risks and vulnerabilities, Maruchek et al. (2011) examine product safety issues in five industries that are increasingly globalising their supply chain using operations management theory. In previous work, Lee and Whang (2005) proved the use of operations management principles as a useful technique in tackling supply chain safety-related risks. The essay identifies four areas where techniques can be used to provide innovative solutions:

- Product lifecycle management
- Traceability and recall management
- Supplier relationships
- Regulations and standards

Maruchek et al. (2011) further specify four areas of focus to effectively reduce the risks associated with supply chain: collaborating with regulatory bodies such as governmental institutions to develop mechanisms that incentivise safety; better tools and methodologies for managing information during the lifecycle of the product from design through disposal; technologies for tracing products across the global supply chain and managing recalls; building supplier relationships as a critical element of a product safety risk management strategy. Maisel (2005) further points to the safety hazards posed by complex new technologies. The paper argues that it is difficult to anticipate these safety risks during development and that they may only be understood when the system is in operation and has fully manifested such risks.

7.5.3 Simplified model for risk reduction in contracts and procurement

Cooper et al. (2005) present a contract risk-sharing scheme suggesting that the general principle applied for optimal risk allocation must be based on allocation to the party best able to manage it, and at least cost. In a basic client and contractor type arrangement, the authors propose that an optimal risk allocation cannot be achieved by passing all the risks onto the contractor but to seek a solution that minimises both, i.e. the total risk management costs. Medda (2007) sees this proposal as sensible, but considerably challenging in achieving the minimisation. This is due to the contrasting results in risk allocation, i.e. optimum risk reduction is not always achieved with the application of this basic principle. It is often the case that the source of the risk has not been well understood, hence there is a small possibility to control the risk efficiently and at low cost.

Narasimhan and Talluri (2009) describe supply chain risks as a disruption or negative outcome triggered by unpredictable events. For effective reduction of contract procurement risks relating to safety, the options are:

1. Risks eliminated or minimised by the risk-holder;
2. Risks transferred to parties most capable of managing them;

If neither is possible,

3. Bearing the risks becomes the only alternative.

It is particularly relevant to examine the complicity of risk bearers, because this is likely to have a strong influence on how far other actors should go in providing them with protection. Busby (2008) makes a case for an explicit analysis of complicity in parallel with normal processes of risk assessment, and proposes a framework for this analysis. The conclusion is that the analysis has to be formative rather than

summative, but that it could provide a useful way of exposing differences in the assumptions of various actors about agency and responsibility.

Eriksen and Jensen (2010) examine an important question: 'Is it possible to design contracts concerning payment mechanisms and financial instruments for transport infrastructure that will stimulate social efficiency and optimal allocation of risks between parties?' A fuzzy model using a company's procurement experiences as a way of implementing organisational learning to improve procurement decisions is presented in Chao and Hsiao (2012). The paper identifies performance metrics such as safety and health as fundamental to the development of decisions on contracts to suppliers during construction risk management. Further, Chao and Hsiao (2012) claim that the use of a fuzzy model determines the contractual arrangements through which the project realises and fulfils its risk reduction goals.

However, common sense suggests that a rational technique could be formulated that would ensure effectiveness with the current broadly practised techniques. A paradigm shift approach is not practicable. Due to the different techniques and complexities introduced by hybrids of safety contracts, the process for effective contracts that consider budget constraints on any safety-related project must look to simplify and enhance existing practice. The competence of suppliers must play a major role before procurement or contract approval. The client must only procure articles from suppliers who are demonstrably competent in the management of engineering services or products.

Considering the key influences on effective risk reduction, an extension of a readiness framework to incorporate the contracts or procurement is provided in Figure 58. The risk readiness concept introduced in Section 7.4 provides a basic template for safety risk assurance that can be used to assess a supplier (or partner in the case of partnerships) prior to procurement or contractual agreements.

Figure 58 introduces a process flow using the risk reduction readiness concept to support contractor competence evaluations and subsequently determine and support approval of suppliers. The risk readiness contract evaluations provided in Figure 58 are tailored to suit a generic safety-related railway project and incorporate the key conditions of a typical contractual relationship. The approach provides the required support for procurement on safety-related projects.

Table 26: Safety contract evaluations

Elements of safety contract evaluation	Description	Objective
Business Evaluation	Business governance, financial stability, project insurance and ownership of the contracting organisation	Addresses basic quality and safety standards. Used to as initial evaluation to retain contractors that can deliver on significant tasks
Technical Evaluation	Compliance with applicable technical and functional requirements for the work-scope	Confirm that the supplier is competent to provide the services that comply with functional standards. In railway applications this typically covers design, modify, manufacture, overhaul, refurbish and service.

Elements of safety contract evaluation	Description	Objective
Assurance Evaluation	Safety assurance, which includes operational risk reduction and safety case, project assurance including site work, systems maintainability and availability.	Undertaken to ensure maintenance of an incident-free railway prior to obtaining the relevant authorisation to operate on the railway network.

Functional experts within the organisation undertake detailed elements of the evaluation process. In practice, an organisation's commitment to contracts follows the competency evaluation. However, prior to any contract agreement, some organisations may request that the hazards associated with the tasks are identified and a gap analysis is undertaken of the supplier's ability to deal with these hazards. For novel technologies or projects, the uncertainties of these evaluations are increased as a result of the unknowns that are associated with the novel technology.

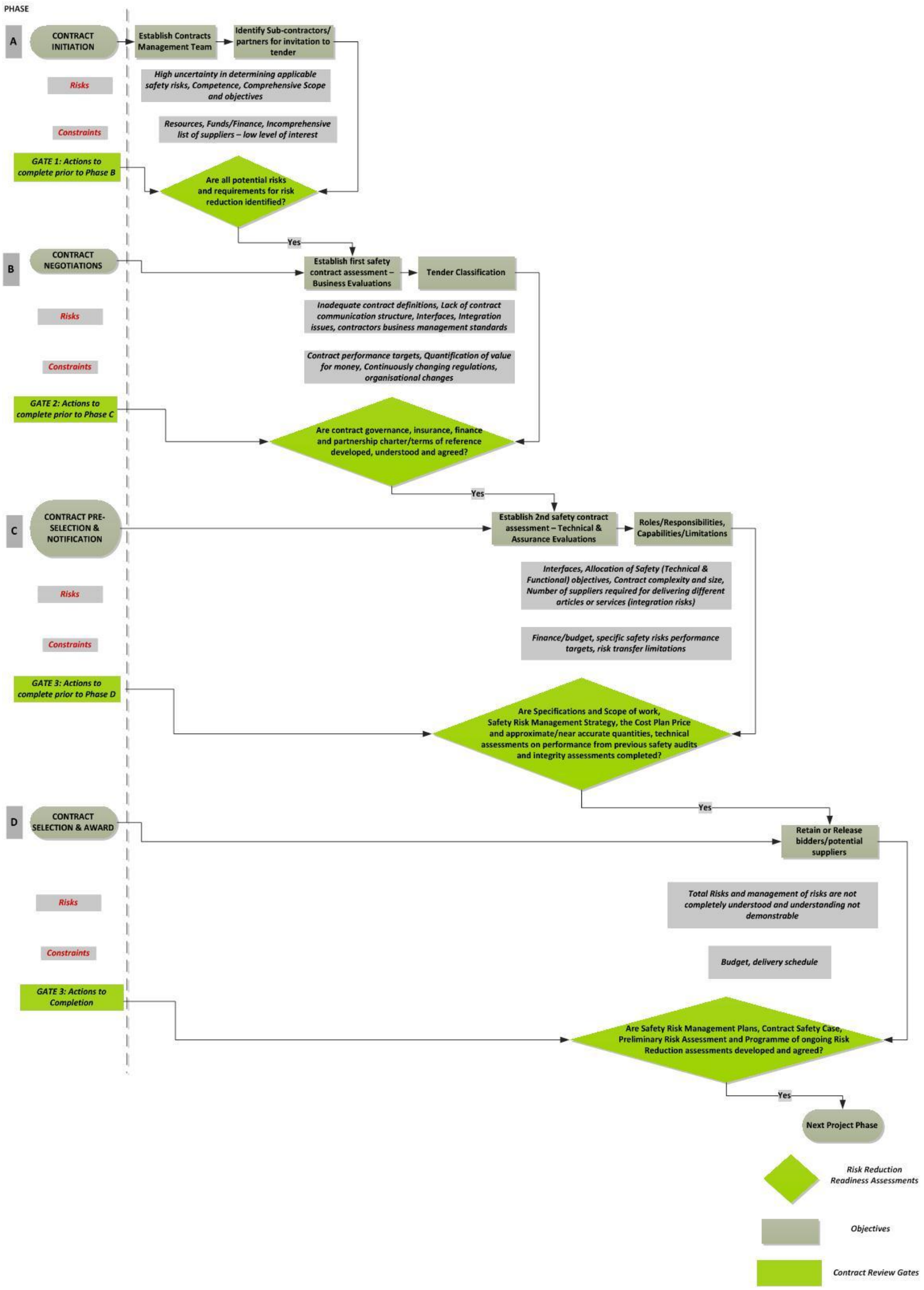


Figure 58: Risk Reduction Readiness (R^3) contract evaluations

7.6 Evaluation and Application of Techniques for Selecting Among Competing Risk Reduction Strategies

Railway operators and infrastructure owners are increasingly required to enhance services by implementing the best options for optimising risk reduction. In practice, the 'As Low As Reasonably Practicable' (ALARP) framework for risk reduction in the railway industry is a challenge that is compounded by decisions that must be made on a finite number of risk reduction options within specified budgets.

7.6.1 Targeting likelihood of first occurrence for risk reduction

In Chapters 5 and 6, this study used the fundamental principles of risk reduction to comprehensively categorise railway risk reduction measures as preventive or protective with examples of their practical application. However, following on from the previous chapters, this section's consideration of optimality seeks to incorporate all risk reduction benefits in line with the concept of 'amount of removed risk from a risk reduction option' and addresses the key challenges (identified in Section 6.7) of selecting risk reduction options. The risk-reduction framework must employ preventive and protective measures in a cost effective manner. The rational approaches introduced in Chapter 7 address some of these requirements for optimised risk reduction; the decision support system requires a method that considers additional cases such as the mutual exclusivity of options for risk reduction within budget constraints.

Let us consider a practical example for the Collision Between Trains (CBT) accident, its contributory factors and possible risk reduction measures. The contributors are mutually exclusive failure modes resulting in the event.

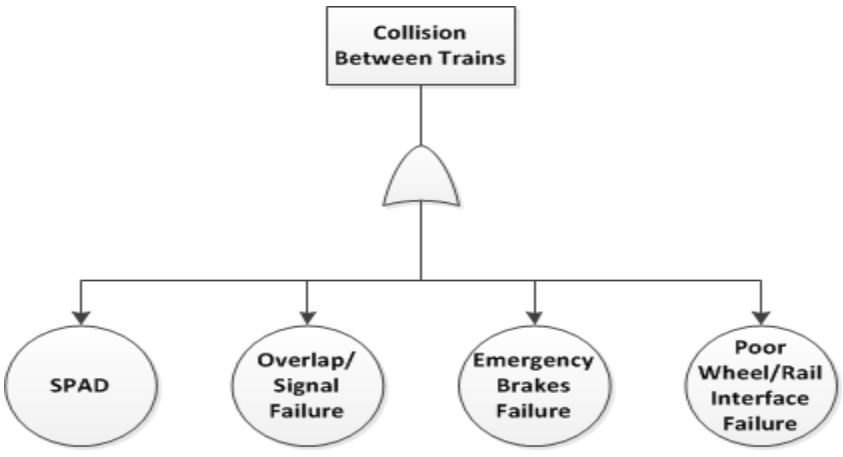


Figure 59: Contributors to Collision Between Trains

The commonly accepted risk of failure equation, as defined in Henley and Kumamoto (1981) is $K = p_f C$ i.e. the product of the probability of the contribution being realised (or failure) p_f and the loss C given

that the failure or contribution occurs. Todinov (2006) proposed a model that gives the risk (in this case the risk of top event materialising) as a function of several mutually exclusive failure modes, each characterised by a constant hazard rate λ_i and consequence, C_i. The expected value of the potential losses from failure (the risk) on a finite time interval with length 'a' is:

$$\overline{C} \equiv \mathrm{K} = (1 - \exp[-(\lambda_1 + \cdots + \lambda_M)a]) \text{ x } \sum_{k=1}^{M} \frac{\lambda_k}{\lambda_1 + \cdots + \lambda_M} \bar{C}_{(k|f)} \qquad (7.6)$$

where *M* is the number of failure modes, *k* = 1, 2,.....,*M* and the sum, $\overline{C_f} = \sum_{k=1}^{M} \frac{\lambda_k}{\lambda_1 + \cdots + \lambda_M} \bar{C}_{(k|f)}$ are the expected losses, given that failure has occurred. Equation 7.6 provides a means of calculating how much risk is reduced by minimising the hazard rate of each individual failure mode. This method is particularly important in cases of systems with multiple contributors (failure modes) to the system failure. Equation 7.6 expresses the fact that the contributors to system failure, each with hazard rate λ_i are competing to fail the system but only the first failure mode to materialise is actually failing the system. In such cases such as the Collision Between Trains with its contributors (Figure 59), the risk of failure is influenced by the failure frequencies of all failure modes but the risk of the top event is actually controlled by the first failure mode to be realised. To illustrate this point, let us assume that the four contributors to Collision Between Trains have the following parameters (Table 27):

Table 27: CBT failure parameters – for illustrating risk reduction based on first occurrence

Contributor (Failure Mode)	Hazard/failure rate (λ)	Consequence (£ x10^4)
Signal Passed At Danger (SPAD)	1.0	100
Overlap/Signal failure	0.1	1000
Emergency Brake failure	0.5	200
Poor Wheel/Rail Interface failure	0.2	500

Then the table of contributors, failure rates and associated costs shows that the consequence of any accident from the Overlap/Signal failure is considerably more than each of the other contributors. However, the risk of the Collision Between Trains accident will be dominated by the SPAD. This is the failure mode that is likely to fail the system. By targeting the risk reduction effort to reduce the contribution from the SPAD, the likelihood of collision between trains is reduced.

7.6.2 Selecting between measures (based on hazard rates and consequence)

Now each major accident contributor is assigned risk reduction measures that potentially reduce the risk of realising the contributor and subsequently, the major accident. These risk reduction measures are given in Table 28.

Table 28: CBT risk reduction measures

Risk Contributor	Risk Reduction Measures	Category (Preventive or Protective)
SPAD	Emergency Timetables	Protective
	Train Warning Systems	Preventive
	Speed Restrictions	Preventive
	Driver Training	Protective
	Crash Worthiness (CEM)	Protective
Emergency Braking	Replace Brake Controllers	Preventive
	Inspection and Testing	Preventive
	Speed/Brake failure alarms or detection systems	Preventive
Poor Wheel/Rail Interface	Vegetation Management Programme	Protective
	Weather forecasting	Preventive
	On-board sanding	Preventive
Overlaps/Signals	Extend overlaps	Preventive
	Incident Plans	Protective
	Signal Modifications	Preventive

If our overall objective is to minimise or eliminate the risk of Collision Between Train accidents, then the probability of realising any of the contributors must also be minimised or eliminated using the measures in Table 28.

If the preventive-first approach is followed (as generally practiced), without considering the hazard rates of the separate failure modes, an application of the measures to reduce or eliminate the likelihood of the accident potentially offers us the following possible measures:

- Replace brake controllers
- Weather forecasting or predictive systems
- Extend overlaps
- On-board sanding
- Inspection and Testing
- Train Warning Systems
- Speed Restrictions
- Speed /Brake failure alarms or detection systems
- Signal modifications

In any combination, the above preventive measure can only satisfy a reduction of hazard rates from the Equation 7.6. The potential loss given the realisation of the contributors to the accident can only be reduced by protective measures:

- Driver Training
- Emergency Timetable
- Vegetation Management Programme

- Incident Plans
- Crash Worthiness (CEM)

In real-life scenarios, the conventional method of selecting the preventive measures only is unlikely to realise the maximum risk reduction. Furthermore, when budget constraints are introduced or play a major part in the selection of risk reduction measures, the typical practice of reducing the likelihood of the accident or other conventional methods based on engineering judgement are at best, ineffective. A method that optimises the risk reduction within the available budget will potentially have to fully consider all measures, preventive and protective.

Considering that each risk reduction measure will have its own cost, the requirement is to distribute the resources (risk reduction measure and associated costs) in such a way that the overall goal of minimising the risk of Collision Between Trains is enhanced within specified budgets.

The combination of all relevant measures in the analysis is attributed to the comprehensive work in Chapter 5 and 6 and Equation 7.6. The choice of risk reduction measure to achieve the maximum effect is significantly influenced by the available budget and how the contributions to the accident are targeted and managed. Consequently, it is especially important that considerations of maximum risk reduction with budget constraints reflect the complete benefit of all measures, preventive and protective, during analyses, evaluation and selection of measures.

The following conclusions can now be made regarding optimising risk reduction within a fixed budget:

- Hazard rates for the contributors to the accident must also be addressed in the overall risk reduction exercise
- Maximum risk reduction within budget constraints can only be achieved if the application limitations and strengths of individual risk reduction measure are comprehensively understood for the particular application scenario
- A combination of Preventive and Protective measures must be implemented for degraded and abnormal operations. This is particularly relevant to incidents or failure scenarios where there is a chance of preventing further accidents or failures.

Chapter 8 Optimal Budget Allocation method for achieving Maximum Risk Reduction

By using the concept '*amount of removed risk by a risk reduction option*', the problem of optimal allocation of a fixed budget, among a finite number of risk reduction options in the railways industry, can be reduced to an optimisation problem from dynamic programming. This chapter proposes the introduction of a dynamic programming technique for optimal risk reduction in the railway industry. For *n* risk reduction options and size of the available risk reduction budget *B* (in thousands pounds sterling), the worst-case running time of the proposed algorithm is O(n x (B+1)). This makes the proposed method a very efficient tool for solving the optimal risk reduction problem in the railway industry.
The optimal solution even for a relatively large number of options has been achieved within a very short time, which makes the developed software a very efficient decision support tool for the railway industry.

This chapter solves the optimal budget allocation problem that supports the maximum risk reduction case presented in this thesis by:

- Defining the maximum risk reduction problem
- Applying the dynamic programming method to a number of known results from test cases to validate the model

8.1 The maximum risk reduction problem

In the apparent absence of an adequate definition of the optimisation of risk reduction within a fixed budget practised on the railways, a mathematical illustration is presented below:

Let us consider a set of risk reduction options from $1 \dots \dots \dots n$ with benefits,
$\varphi_1(x), \varphi_2(x), \dots \dots \dots \dots \dots \varphi_n(x)$

For each risk reduction option $\varphi_1(x)$ where $\varphi_i = 1 \dots \dots \dots \dots n$ are known functions.

Find an optimal vector, $x^* = \{x_1^*, x_2^*, \dots, x_n^*\}$ such that

$\sum_{i=1}^{n} \varphi_i(x_i^*)$ is a maximum, given the budget constraint

$$\sum_{i=1}^{n} x_i^* \leq B \tag{8.1}$$

where *B* is the available budget. The optimisation of risk reduction options within a fixed budget is then defined below as: Maximise

$$\sum_{i=1}^{n} \varphi_i(x_i^*)$$

given the budget constraint:

$$\sum_{i=1}^{n} x_i^* \leq B \tag{8.2}$$

Considering ALARP and tolerability requirements, the problem can be further represented to capture and illustrate risk reduction optimisation within a fixed budget in Figure 60 (the ALARP triangle in reverse to reflect the parameters and how they can be linked together)

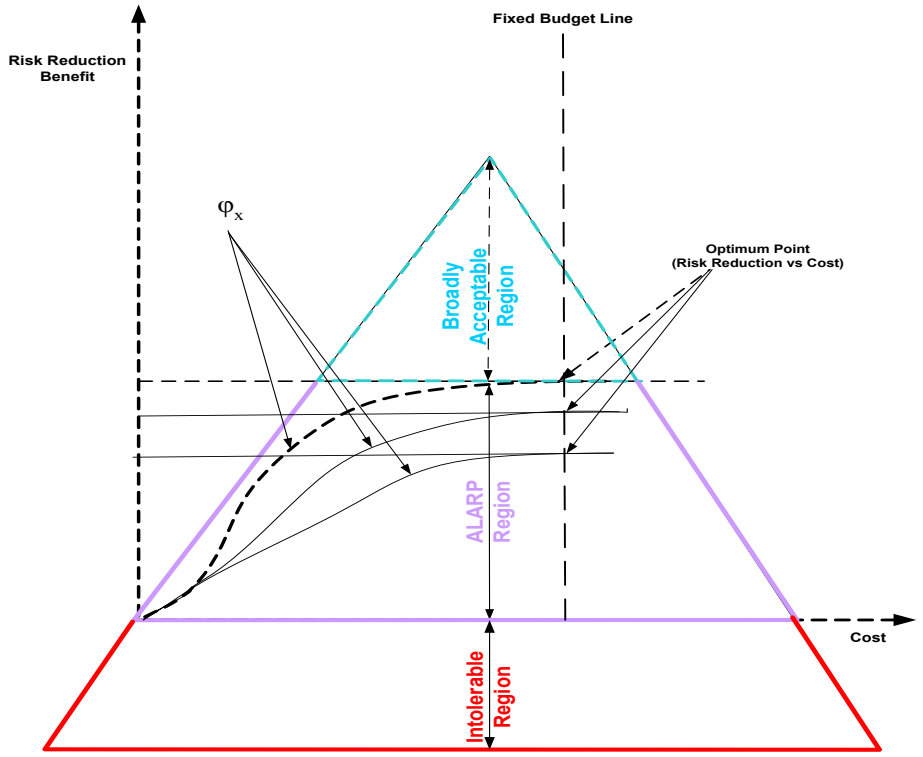


Figure 60: Optimum risk reduction within fixed budget

8.2 Evaluation and Application of Dynamic Programming as a Technique for Risk Reduction Decisions

This section presents the fundamental application principles and application examples of dynamic programming (DP). This is a powerful tool that, in general, results in solutions for a variety of complex combinatorial optimisation problems.

8.2.1 Review of alternatives to dynamic programming

The current application of the cost-benefit technique as a decision support tool for determining the best options for risk reduction is inadequate (Elvik, 2001). The limitations of CBA as a widely accepted technique on the railways have been comprehensively discussed in previous chapters.

Advocates for alternative techniques to cost-benefit analysis include Li et al. (2009) and An et al. (2011). However, these studies have exposed the inadequacies of applying basic economic theories to the transport industry (e.g., Flyvberg et al., 2003). The Expected Utility Theory, has been discussed comprehensively in Chapter 4.

Analytical hierarchy process is another technique, which requires the use of a pairwise comparison matrix and eigenvector to specify weights higher than a specified threshold (Ramanthan & Ganesh, 1995); (Saaty, 1988). However, the AHP technique does not adequately support the decision-maker in choosing alternatives that have higher weights than the threshold and is unsuitable for making more than one choice when multiple alternatives are provided (Ghazinoory et al., 2006). Other proponents of alternatives to the cost-benefit approach have demonstrated the application of different optimisation techniques in addressing risk reduction within budget constraints: (Rashid & Hayes 2011); (Cagno et al. 2001); (Persaud & Kazakov 1994); (Khisty & Mohammadi 2001); (Lindhe et al. 2010); (Ozmir and Demirel 2012); (Sato 2012); (Caputo (2012).

These studies apply multi-criteria optimisation methods such as AHP, Simulated Annealing, Tabu Search, Genetic Algorithms, and combinations of these, with varying success. Limitations to the use of these approaches are well documented (Pirlot, 1996); (Olson 1988); (Hey 1995); (van Laarhoven et al. 1992); (Johnson et al. 1991); (Mitchell 1996); (Aven & Korte 2003); (Fukuba & Ito 1983) and (Aven & Kristensen (2005). Heuristic methods do not guarantee that the solutions found will be optimal.

Basso & Peccati (2001) through a comprehensive analysis, demonstrate that optimal resource allocation problems are NP-hard problems. Horowitz & Sahni (1974); Balas & Zemel (1980), supported by studies undertaken on the suitability of optimisation techniques have concluded that the solution of optimal resource allocation is best addressed by using dynamic programming (Bjorndal et al. 1995).

8.2.2 Definitions and Applications of Dynamic Programming

For a good introduction to the solution of problems lying within the domain of dynamic programming, we refer to the basic approaches introduced by Bellman (1957). Dynamic programming is based on the principle of optimality which considers that an optimal policy has the property that, **whatever the initial state and initial decision are, the remaining decisions must constitute an optimal policy with regard to the state resulting from the first decision**. Bellman considers a simple multi-stage allocation process that possesses many of the elements common to a variety of practical problems including the control of engineering systems. This straightforward, formulation presents the fundamentals to dynamic programming as an effective computational analysis technique for risk reduction within a fixed budget.

To illustrate the basic idea of the dynamic programming, we introduce the functional equation approach. The optimisation of the resource allocation related to a multi-stage allocation process can be illustrated by considering a two stage process.

Bellman defines the function $f_N(x)$ as the maximum return obtained from an N-stage process starting with an initial quantity x, for $N = 1, 2, \ldots, and\ x \geq 0$.

$$f_N(x) = \text{Max}\, R_N\ (x, y, \ldots., y_{N-1}),\ N = 2, 3, \ldots \quad (8.3)$$

with

$$f_1(x) = \text{Max}\ [g\ (y) + h\ (x - y)] \quad \text{where } 0 \leq y\ \leq x \quad (8.4)$$

where g and h are the known functions. For a two-stage process, the total return will be the return from the first stage plus the return from the second stage giving us a total of $ay + b\ (x - y)$ left to allocate. The remaining amount must then be used in the most effective way to obtain a two-stage optimisation. For the two-stage process resulting from the initial allocation of y, the expression is:

$$R_2(x, y, y_1) = g\ (y) + h\ (x - y) + \ f_1(ay + b\ (x - y)) \quad (8.5)$$

The recurrence relation is also provided as:

$$f_2(x) = \text{Max}\ [g\ (y) + h\ (x - y) + \ f_1\big(ay + b\ (x - y)\big)] \quad (8.6)$$

where and a and b are known constants satisfying the condition $0\ \leq a, b < 1$. By applying the same argument for the N-stage process, the basic functional equation is represented as:

$$f_N(x) = \text{Max}\ [g\ (y) + h\ (x - y) + \ f_{N-1}\big(ay + b\ (x - y)\big)] \text{ where } 0 \leq y\ \leq x. \quad (8.7)$$

for $N \geq 2$ with $f_1(x)$ defined as $f_1(x) = \text{Max}\ [\text{g (y)} + h\ (x - y)]$ where $0 \leq y\ \leq x$

The solution of the computation will consist of a tabulation of the sequence of functions

$\{y_k(x)\} and\ \{f_k(x)\}$ for $x \geq 0, k = 1,2, \ldots..$

$\bar{y} =\ y_N(x),$

$\bar{y}_1 =\ y_{N-1}(a\bar{y} + b\ (x -\ \bar{y})),$

$\bar{y}_2 =\ y_{N-2}(a\bar{y}_1 + b\ (x_1 - \bar{y}_1)),$

.

.

.

$\bar{y}_{N-1} = y_1(a\bar{y}_{N-2} + b\ (x_{N-2} - \bar{y}_{N-2}))$, where $(\bar{y}, \bar{y}_1, , \ldots \ldots . , \bar{y}_{N-1})$ is a set of allocations that maximises the total N-stage return.

Eddy (2004) summarises that, the DP algorithm consists of 4 primary steps:

1. A recursive definition for the optimal solution
2. A look-up table to store the optimal solution for the sub optimal problem;
3. A bottom-up approach which starts from the simplest sub-problem to fill the look-up table;
4. A track-back method to reconstruct the final optimal solution to the problem.

The wide range of applications using dynamic programming that has been used in research and industry for solving optimisation problems includes optimal resource allocation, which is close to the topic of this thesis. Other applications that frequently feature in industry and research include complex decision-making problems under uncertainty such as biological sequence manipulation, risk management, operations research, control and information theory, artificial intelligence and reliability analysis. In addition, Dreyfus (2010) provides a comprehensive list of dynamic programming application areas.

As identified in Arunkumar (1975), Gessford and Karlin (1958) were among the first to employ a dynamic programming model to obtain the form of optimal release rules for an infinite dam over finite periods of time, allowing the probability distributions of the input variables and the convex cost function to depend on time. Tsitsiklis and Van Roy (1999) illustrate its use in solving the classical optimal stopping position problem. Gitirana (2005) introduces a decision support system using dynamic programming for managing railway embankment hazards, based on concepts of unsaturated soil mechanics and hydrology. The dynamic programme constitutes an algorithm for slope stability analysis (Safe-DP) and is incorporated into an existing weather-related geo-hazard model. The latter is used to efficiently assess railway embankment hazards based on factors of safety and probabilities of failures that are computed by applying soil property variability and case scenarios.

Baker (1980); Pham and Fredlund (2003) demonstrate an unusual yet efficient application of dynamic programming to slope stability analysis. The results obtained were compared against findings from several well-known limit equilibrium methods. The comparisons demonstrated the superiority of dynamic programming compared to limit equilibrium methods. The factors of safety derived by the use of dynamic programming were shown to be slightly lower. However, as the Poisson's ratio approaches 0.5, the computed factors of safety from the dynamic programming method and the limit of equilibrium method resulted in similar outcomes. By applying the tools of dynamic programming to theoretical economics, specific case of unbounded returns, Alvarez and Stokey (1998) show that the basic existence, uniqueness, and convergence of the dynamic programming solution hold when the return function is

homogeneous of degree $\theta \leq 1$ and the constraints are homogeneous of degree one. This particular work proves that dynamic programming hold for homogeneous unbounded problems.

Dynamic programming is widely applied in developing speech recognition systems in order to address the problem of the time alignment between speech segment and synthesised speech artefact. Most commercially available speech recognisers and many of the systems developed in research laboratories are discussed in Silverman and Morgan (1990).

In practice, a typical engineering optimisation challenge provides a variety of application constraints such as technical and functional requirements, cost limitations and resource allocation issues. Dynamic programming has been proved to be an effective tool for providing solutions to such problems. A good example of this application of dynamic programming is that presented by Tung et al. (2013). A DP model is designed for thermal generating units which include operating cost as the most imperative parameter to optimize. Unit output ranges are extracted and computation revealed an optimisation of operating cost that corresponds to various load demands. The load is increased in small step sizes and number of unit combinations to be derived for particular plant output is substantially reduced. As a result, the computation time is significantly reduced compared to direct enumeration techniques. The paper presents simulation studies that reflect different combination units against different load demands and the effective minimisation of operating cost for the total load.

In advanced engineering applications of dynamic programming, the approach in Bhardwaj et al. (2012) in optimising power system unit commitment further demonstrates the wide ranging capability of DP. A unit commitment problem typically involves scheduling on/off states of generating units which minimises the costs of operating, start-up, and shut-down for a specified system under operating constraints. In addition to fulfilling a significant number of constraints, load demands, spinning reserves requirements and time thresholds must be achieved at a minimum cost. This detailed study presented definitive solutions to the optimisation problem by using dynamic programming. Optimisation of a road network is undertaken by a dynamic programming model that evaluates the shortest path in the road network (Shehzad and Shah 2009).

8.2.3 Limitations of Dynamic Programming

The challenges of applying dynamic programming to develop sequential decision-making on complex processes such as real-time operation adaptive signalling control are outlined in Chai (2009). The work is based on the premise that applying the classic dynamic programming technique to controlling traffic signals at isolated intersections and in distributed traffic networks increases computational burden. The work suggests that an approximate dynamic programming (ADP) technique for such difficult

computational problems can be employed as a second-best option. This specific application is one of the published few applications of dynamic programming in the transport industry. Similarly, an earlier transport industry analysis, Henry et al. (1983) found that the memory requirements for problems with very large state space such as a traffic section with four links proves computationally intractable in dynamic programming.

Bellman and Dreyfus (1962); Powell (2007) point to the computational limitations caused by the 'curse of dimensionality' that makes dynamic programming impracticable for use on transport systems applications where risk reduction within a specified time frame (e.g. safe stopping functionality) is a primary requirement. The paper considers this impracticality for some systems applications a fundamental flaw considering the limited time window available for evaluating and implementing a safety-related decision. In clearer terms, this acute problem in empirical applications of dynamic programming means that the time required for computing a solution exponentially increases with the number of possible decisions or states. However, despite this specific limitation, the exponential growth of developments in information technology has resulted in more powerful computers capable of performing huge number of operations per second. These significant improvements in information technology have made the application of dynamic programming viable for problems with higher dimensionality. With a view to proving the validity of dynamic programming solutions, Sniedovich (1978) developed a sequential decision model to define the principles of optimality and to validate solutions from dynamic programming functional equations.

8.3 Description of the proposed method and algorithm

Let S be the set of all available n risk reduction options i=1, 2..., n for a particular major risk in the railway industry. As a measure of the effectiveness of each risk reduction option, we postulate the amount of removed risk. This is the expected cost of prevented accidents, delays, fatalities, injuries etc. expressed in monetary terms. Each risk reduction measure i, (i=1, 2..., n) is characterised by the amount of risk that it removes after its implementation. Each risk reduction measure i, (i=1, 2..., n), is also characterised by its cost of implementation.

Each risk reduction option cannot be selected more than once. As a result, each option from the set S of all available risk reduction options can either be accepted or rejected.

The task of optimal allocation of the fixed budget reduces to determining the optimal subset of risk reduction options, whose total sum of removed risks is maximum and whose total cost does not exceed the available risk reduction budget B. This problem can be formally presented as:

Maximise:

$\sum_{i=1}^{n} \varphi_i(x_i^*)$

Given the budget constraint: $\sum_{i=1}^{n} x_i^* \leq B$

Where the risk reduction benefit, φ_i for each option, x_i is subject to the available budget, B.

Considering the magnitude of the implementation costs for the risk reduction options in the railway industry and the magnitude of removed risks, we can safely assume that the costs and the amount of removed risk can always be expressed as relatively small integer numbers. In the application related to the railways, the removed risk and the cost of implementation are expressed in thousands of pounds sterling.

Thus, removed risk of 65 and by a risk reduction option which costs 27, stands for removed risk worth £65000 by an option whose cost of implementation is £27000. It is also assumed that the available budget can also be specified in thousands of pounds sterling, as a relatively small integer number.

As a result, the problem of optimal allocation of a risk reduction budget in the railway industry has been reduced to a combinatorial optimisation problem involving relatively small integer numbers only. This problem can be solved by using a dynamic programming technique also used for solving the 'knapsack without repetition problem' (Dasgupta et al., 2008). Although dynamic programming techniques have been known for a long time, to the best of our knowledge, these methods have been applied for the first time in this thesis to solve the problem of optimal risk reduction in the railway industry.

The advantage of the dynamic programming (Bellman 1957), consists in the fact that it finds solutions to sub-problems increasing in size, stores them in the memory, and describes the solution of each sub-problem in terms of already solved and previously stored solutions of smaller sub-problems. As a result, **sub-problems are solved only once**, which makes the dynamic programming significantly more efficient than a brute-force method based on the enumeration of all possible subsets in the set S. The number of all possible subsets in a set S with *n* elements is 2^n and the computational time of a brute-force method based on the enumeration of all possible subsets rises dramatically with increasing the number n of risk reduction options. Here is the description of the algorithm in pseudo-code:

8.3.1 Algorithm 1 (in pseudo-code)- Building the dynamic risk reduction table.

Initialising array x [][] with zeroes in the first row and in the first column.

for i=1 to n do

for j=1 to B do

```
{
  cur_budget=j;
  if(c[i]>cur_budget) then  { x[i][j]=x[i-1][j]; trac[i][j]=0; }
        else
        {
        rem = cur_budget-c[i];
        tmp = rr[i]+x[i-1][rem];
        if(x[i-1][cur_budget]>tmp) then {
                                          x[i][j] = x[i-1][j]; trac[i][j]=0;
                                        }
              else {
                     x[i][j]=tmp; trac[i][j]=1;
                   }
        }
}
```

The algorithm works as follows. The solutions of the sub-problems are kept in the array x[][]. The information necessary to restore the optimal solution is kept in the array trac[][]. The size of the x[][] array is (n+1) x B elements. The first row of the array x[][] corresponds to zero number of selected options in the optimal set P; the first column of the array x[][] corresponds to zero budget.

The sub-problems are defined by the size of the current budget which varies from 1 to B units. The cost of the ith risk reduction option is compared with the value of the current budget and if it is greater than the current budget, the ith risk reduction option is not included in the optimal set, which is reflected by the zero value in the trac array (trac[i][j]=0). In the case where the current budget is greater than the cost of the ith risk reduction option, a decision is taken whether to include the ith risk reduction option or not.

Initially, the statement 'rem = cur_budget-c[i];' determines the amount of remaining budget if the ith risk reduction option is included. The sub-problem marked by x[i-1][rem] however has already been solved and its solution has been recorded in the x[][] array. The entry x[i-1][rem] gives the maximum amount of removed risk within budget equal to 'rem' and for available risk reduction options from 1 to i-1. Consequently, the solution of the sub-problem does not need to be obtained again; it can simply be read out from the x[][] array. The amount of risk removed by the ith risk reduction option is rr[i]. Consequently, the maximum amount of removed risk for budget cur_budget=j, if the ith risk reduction option is included, is given by 'tmp = rr[i]+x[i-1][rem];'. If the ith option is not included in the optimal set P, the maximum amount of removed risk within the budget cur_budget is given by x[i-1][cur_budget].

Consequently, the decision whether to include the ith risk reduction option in the optimal set or not depends on the outcome of the comparison made in the statement: if(x [i-1][cur_budget]>tmp)

If 'x[i-1][cur_budget] > tmp', not including the ith risk reduction option yields greater amount of removed risk and the entry 'trac[i][j]=0' in the track[][] array is set to zero, which indicates that the ith risk reduction option has not been included in the optimum set of options P. The maximum amount of removed risk is equal to the maximum amount of removed risk within the current budget 'j', for i-1 total number of available options. This maximum however has already been computed and is in the array x[][]; this is the entry x[i-1][j].

If 'x[i-1][cur_budget] < tmp' then including the ith option yields greater amount of removed risk and the entry in the array trac[i][j]=1; is set to one which indicates that the ith risk reduction option has been included in the optimal set P. The maximum amount of removed risk is equal to:

x[i][j]=tmp; or x[i][j]= rr[i]+x[i-1][rem];

In words, the maximum amount of removed risk is equal to the removed risk from including the ith risk-reduction option plus the maximum amount of removed risk for i-1 available options within the remaining budget 'rem'. The optimal set of options is restored by the next algorithm in pseudo-code.

8.3.2 Algorithm 2 - Restoring the optimal set of risk reduction options from the dynamic tables.

Initialise all entries of the solution [] array with zeroes.

```
cur_bud=B;
cur_opt=n;
tmp=trac[cur_opt][cur_bud];
 while (cur_opt > =1 ) do
        {
           if (trac[cur_opt][cur_bud]=1)  then   {
                                                    solution[cur_opt] = 1;
                                                     cur_bud=cur_bud - c[cur_opt];
                                                      cur_opt = cur_opt - 1;
                                                    }
          else  cur_opt=cur_opt-1;
        }
```

The algorithm starts with the entry trac[n][B] of the track[][] array, which corresponds to a full budget B and all n available risk reduction options. If the n-th options has been included in the optimal set, this will be indicated by a non-zero entry in the trac array (trac[n][B]=1). In this case, the solution array marks the n-th option as 'included' in the optimal set P, by the statement 'solution[n]=1'. The current budget is then reduced by the statement 'cur_bud=cur_bud - c[cur_opt]' with the cost of the current (n-th) option. The current option to be considered should now be the n-1st option. This is ensured by the statement 'cur_opt = cur_opt-1'.

If the n-th option has not been included in the optimal set, this will be indicated by a zero entry in the trac-array (trac[n][B]=0). In this case, the current budget is not altered because no cost has been incurred for implementing the n-th risk reduction option.

The process of considering the options in reverse order continues until the first option is reached. At this point, the entries of the solution array will contain '1' for the options which have been included in the optimal set P. The running time of Algorithm 1 for building the dynamic tables is determined by the two nested loops:

for i=1 to n do

for j=1 to B do

{ ..... }

which contain a set of operation that are executed in constant time. The maximum number of steps after which Algorithm 1 will terminate is $n \text{ x } B$. The maximum number of steps for Algorithm 2 is n because after each iteration of the while-do loop, the number of options is reduced by 1. As a result, after at most n steps, Algorithm 2 will terminate. The total number of steps is therefore $\text{x } B + n = n \text{ x } (B + 1)$. The worst-case running time of the algorithm for optimal allocation of a risk reduction budget is therefore $O(n \text{ x } (B + 1))$.

This algorithm has been tested on a large number of standard data sets with known solutions and presented in Section 8.4. For each of the data sets the algorithm reproduced the correct solution.

8.4 Solved test cases by the proposed method, featuring optimal budget allocation to achieve a maximum risk reduction in the railway industry

In this section, a case study of a railway line section has been used to demonstrate the effectiveness and accuracy of the dynamic programming optimisation technique for a major renewal project. The accident data set has been extracted from a major renewals project on a 70km railway line with 34 stations, operating 33 - 35 trains a day. The railway line operates at an average speed of 60 to 70km/h with 54 million journeys annually. Three major railway accidents for the line are used as test cases for the optimisation algorithm using different budget parameter settings. The test cases are:

- Test Case 1 (relatively small number of standard data sets) – Platform Train Interface accidents with 20 risk reduction options, associated with removed risks at variable costs.
- Test Case 2 (medium sized data set) – Derailment accidents with 42 risk reduction options, associated with removed risks at variable costs.
- Test Case 3 (large data set) – Train Collision accidents with 81 risk reduction options, associated with removed risks at variable costs.

In addition, Test Case 4 is based on data from a renowned train systems manufacturer and demonstrates that the dynamic programming approach to budget allocation converges to a global optimum, relevant and practicable considering recent budget cuts on railways projects worldwide. This is further proven by analysis of the results in Section 8.5.

8.4.1 Test case 1 – Platform Train Interface

The study focuses on the major accident risks on the line – Platform Train Interface (Platform-only accidents). For the Platform Train Interface only accidents, 20 available risk reduction options have been identified. The removed risk and cost are given as a multiple of £10000. Table 29 provides details used for computing the optimum risk reduction when budgets are specified.

Table 29: Platform Train Interface – Cost and Removed Risk

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
1	Emergency/incident management systems	100	530
2	Station defect reporting & corrective system	10	35
3	Emergency drills – station staff training	20	67
4	Crowd control procedures & systems	100	265
5	Slip, trip, fall toolkit	10	20
6	Station surface inspections/testing	100	220
7	Platform Edge Doors (half length)	800	1360
8	Audible warnings on platform	100	132
9	Access & egress from incident site	200	260
10	Support from platform supervisors	300	320
11	Painted line warnings/signage	50	530
12	Platform emergency plungers – train stops	400	3900
13	Gap fillers	200	180
14	One-person-operated CCTV systems	1200	6100
15	Stair-nose marking	500	350
16	Station supervisor/personnel training	100	660
17	Re-design/re-build platform	1000	2800
18	Platform lighting (incl. emergency lighting)	550	1300
19	Increased traffic – major events, peak times	1000	1200
20	Enhanced surfaces –platforms	350	410

For different specified budgets, the optimal set of risk reduction options are according to Table 30

Table 30: Risk reduction options after optimisation based on fixed budgets

Budget [x £10,000]	Optimal set of options	Cost of option [x £10,000]	Removed Risk [x £10,000]
2900	1,11,12,14,15,16,17	2900	14870
3300	1,4,6,9,11, 12,14,15,16,17	3300	15615
3500	1,2,3,5,11,12,14,15,16,17,18	3490	16292
4000	1,2,3,4,5,6,8,9,11,12,14,15,16,17,18	3990	17169

8.4.2 Test case 2 – Derailment

The analysis is undertaken for derailment accidents with cost and removed risk information provided in Table 31.

Table 31: Derailment – Cost and Removed Risk

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
1	Replacement of rubber springs	1200	2300
2	Inspection and Maintenance of suspension to prevent incorrectly gauged suspensions in the depot prior to train deployment	1000	4600
3	Improve inspection, testing and maintenance regime for detection of wheel flat and worn wheel failures	1000	4600

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
4	Additional training for route setting personnel	1000	4600
5	Speed restrictions	5000	15000
6	Optimising cab design for driver protection in a collision	6000	55000
7	Traction/power assessment - introduction of systems such as surge arrestors, current limiters etc.	1000	9000
8	Buffer stops	5200	36000
9	Master controller installed in driver's cab for the driver to reduce or apply power to train	6000	9000
10	Review of operational concept/procedures for 'proceed under rule'	1000	900
11	Inspection and maintenance of shoe-gear prior to deployment	1000	900
12	Review programme for structural assessments/surveys - potentially more surveys/assessments introduced to existing programme	1000	1700
13	Structural reinforcements - bridges, embankments	15000	1200
14	Reduced traffic on bridge/structure	10000	4000
15	Programme for assessment and management of workload for train drivers, line controllers, signallers and safety-critical staff	1000	1800
16	Improve inspection and testing of fishplated joints - track	1000	1800
17	Replacement of fishplated joints	10000	2600
18	Repositioning of tripcocks - standard requirement is tripcock positioning 1.5m from front of train	1000	28000
19	EMC studies on trains compatibility with track/signals - monitor interference levels, identification and introduction of relevant immunisation/earthing solutions and potentially further operational railway testing	6000	13000
20	Introduce training and competence management schemes for train crew	5000	7000
21	Introduce injury prevention initiatives e.g. booklets, DVDs and staff briefings	200	5000
22	Review and improve rostering to reduce fatigue	500	14000
23	Unobstructed monitoring of drivers and train despatch and subsequent modifications/amendments to despatch rules (Rules for train despatch reviewed/simplified (procedural change and subsequently, driver training on new despatch rules)	1000	9300
24	Improved management processes for train recovery	1000	5000
25	Introduction of sequential systems of various kinds such as axle counters and other position detector systems etc. (in addition to track circuits to provide redundancy & diversity)	15000	38000
26	Replacement of track circuits	55000	43000
27	Enhanced maintenance/testing such as detailed observation of the track circuit operation and re-adjustment of the track circuit (operating voltages)	6500	13000
28	Introduction of (improved) shunting policy	1000	28000
29	Review and improvement of recruitment and selection processes	1000	14000
30	Examining supervision and monitoring guidelines for operational safety staff, including shunters	1000	7000
31	Trains fitted with incident response kits and additional training for staff to act as quickly as possible in emergency situations	400	14000
32	Crowd control	7000	17000
33	Fire and rescue services	5000	27000
34	Paramedics/medical units (availability of staff trained for train accident scenarios)	5000	27000
35	stronger windows -also minimises risk of object penetration through windows	6000	35000
36	Emergency lighting and signage (illumination of Emergency Door Release mechanisms in	200	900

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
	passenger vehicles)		
37	Provision of hammers for emergency exit	10	3000
38	Track re-alignment to gauge (focus on track stressing & effects)	10000	180000
38	Track inspections - track vehicles	4000	170000
40	Track inspections - track workers	2000	93000
41	Track refurbishment/renewals (including sleeper management programme to reduce gauge spread)	2500	200000
42	Track and conductor rail alignment	3000	35000

Different budgets are specified for achieving the optimal set of risk reduction options and provided in Table 32.

Table 32: Derailment - Risk reduction options after optimisation based on fixed budgets

Budget [x £10,000]	Optimal set of options	Cost of option [x £10,000]	Removed Risk [x £10,000]
3000	7,18,21,22,23,24, 28, 29,30,31, 36,37,38,39,40,41,42	2981	81520
3500	6,7,18,21,22,23,28, 29,30,31,36,37,38,39,40,41,42	3481	86520
4000	6,7,8, 18, 21,22, 23, 28, 29,30,31,37,38,39,40,41,42	3981	90030
5000	6,7,8,18,21,22,23,28, 29,31,34,35,37,38,39,40,41,42	4981	95530

8.4.3 Test case 3 – Collision Between Trains

The number of identified risk reduction options for the risk 'Collision Between Trains' was 81. The risk reduction measures have been listed with the associated costs and risk reduction achieved.

Table 33: Collision Between Trains (CBT) – Cost and Removed Risk

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
1	Improve braking systems	7000	49000
2	Replacement of brake controllers	6000	42000
3	Renewal of brake valves	3000	35000
4	Additional testing and inspection - improve test and inspection regimes (specifically brake systems) prior to deployment	5000	4500
5	Driver training on the use of emergency braking (deadman handle)	1000	12000
6	Introduction of alternative / automatic braking systems to improve availability of braking systems	12000	52000
7	Introduction of brake failure alarms or detection systems	6000	17000
8	EMC studies, monitoring interference levels	1000	900
9	Traction system renewal/refurbishment	5000	5800
10	Improvement of processes/procedures (including driver training)	1000	1700
11	Further/enhanced/additional operational railway testing prior to operations on live track	5000	700
12	Re-assessment of stabling procedures - potentially leading to change in stabling procedures	1500	1600

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
	and subsequently training of depot staff and train drivers		
13	Improve testing and maintenance regime for trainstop, parking brakes for all stabling points	5000	1500
14	Enhanced testing and maintenance regime for spring applied parking brakes to Eliminate/reduce WSF of the spring applied parking brakes	5000	1100
15	Relocation of stabling points - from downslope locations	5500	700
16	Improved communication between line controller and drivers/operators	1000	3400
17	Replace with improved speed sensing equipment	12000	20000
18	SCAT system inspected/tested prior to train leaving the depot - improved SCAT inspection and testing regime	10000	27000
19	Modification of train movement procedures and driver training - improved additional training and driver behavioural studies/assessments	3000	8900
20	Extensive sighting studies to identify potential sighting problems	1000	6100
21	Modification of signalling in line with sighting constraints	40000	13000
22	Change to single stopping positions	5000	11000
23	Introduction and use of in-cab CCTV eliminating/reducing other person induced constraints on stopping positions	30000	13000
24	Introducing train stops in areas where they currently don't exist	7000	16000
25	Introduction of enhanced technology such as radar/alarm systems	7000	11000
26	Additional supervision to check the aspect prior to the reverse movement	1000	18000
27	Track re-alignment to gauge (focus on track stressing & effects of weather on embankment and structures	10000	41000
28	Speed restrictions - side swipe	5000	17000
29	On-board sanding	2000	6000
30	Driver training - braking techniques	1000	12000
31	Notices on slippery routes	1000	3000
32	Alarm/Audible warning of service brake failure prior to brake demand	3000	12000
33	Berth track diversity	20000	31000
34	Speed restriction - Compromised overlaps	5000	17000
35	Overlap studies and potential extension of overlaps	3000	5900
36	Enhance braking performance (See 'Improved braking system' above)	7000	22000
37	Studies on effect of power in trains (especially for the introduction of new trains) and potentially driver training on specific areas of compromised overlaps (controlling trains - traction power management)	1000	3000
38	Driver training – SPAD	3000	18000
39	Train speed restrictions - likely SPAD locations (Signal Sighting)	5000	23000
40	Vegetation management programme - leaf fall (autumn season specific challenge)	5000	35000
41	Fitting of wheel slip protection or Adhesion improvers	2200	12000
42	On-board sanding (see also 'Service Brake Failure')	2000	12000
43	Increased overlap in the design of the signalling system - extension of overlaps	3000	12000
44	Introduction of weather forecasting/predictive systems such as ACAT	500	6000
45	Water jetting and sandite	2000	12000
46	Wheel rim scrubbers	200	1200
47	Anti-icing trains - spraying heated anti-freeze onto the affected areas	4000	6000

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
48	Procedures (also covering changes to operational concept) and subsequent driver and relevant railway driver training	5000	47000
49	Train arrestor assessment and deployment/installation	20000	170000
50	Extend operational testing prior to service for tripcocks, arrestors and SPAD control systems	1000	6000
51	Emergency timetable - contingency plan for dealing with severe disruption (production of emergency timetables and dissemination of timetable information to all personnel especially operational personnel following an accident)	2000	4600
52	Driver training - additional procedures to support drivers (SPAD)	2000	6000
53	SPAD incident plan (immediate detection and action on signals passed at danger to reduce the consequence of failure)	1000	15000
54	Crash worthiness and vehicle interior	21000	86000
55	ATC system introduction	190000	107000
56	New/enhanced interlocking system - route locking system	85000	201000
57	Introduction of automatic signalling systems - minimisation of human error	110000	179000
58	TPWS Train Protection and Warning System	50000	180000
59	Modify signalling to align with sighting constraints	40000	66000
60	Speed restrictions (Adhesion)	15000	65000
61	Additional testing and inspection of wheels and rail (NDT)	6000	12000
62	Tripcock positions to be re-examined and potential relocation/re-installation	5000	24000
63	Exhaustive network survey to identify potential sighting issues	300	600
64	Extend overlaps	3000	19000
65	Additional testing of brakes to determine if brakes are isolated	1000	6000
66	Precautions, procedural modifications and subsequently, driver training for running with isolated emergency brakes	3000	18000
67	Introduction of enhanced braking system - eliminate scenarios where emergency brake signals fail to transmit to brakes (Same as ‘improved braking’ above)	12000	47000
68	Assess the emergency brake performance of trains	300	3100
69	Training for maintenance and test teams	1000	6000
70	Additional operational testing and inclusion in regime for rigorous asset acceptance/approval	5000	8500
71	introduction of advanced radio/comms network across line section	11000	20000
72	Rewiring/refurbishment of existing comms/radio systems	11000	4000
73	Update communication procedure and related procedures for drivers and line controllers	600	4900
74	Modify the train traction system e.g. filters, ICMU (Interference Current Monitoring Unit)	1000	6000
75	Emergency accident/incident plans	1000	7000
76	Incident team on site - trained incident stations staff availability	3000	8700
77	Training for drivers and incident centre personnel	1200	4700
78	Training for local emergency medical team on train accidents/incidents	600	4800
79	Additional procedures and subsequently, Driver and Signal Operator training - observation that wrong route is set prior to proceeding past signal	1000	7100
80	Audible warning systems – trains	1100	4700
81	Points machine failure - new/enhanced point machines with ‘route holding diversity’	11000	10000

Using the 'Train Collisions' data set, different budgets are applied for achieving the optimal set of risk reduction options and provided in Table 34.

Table 34: Collision Between Trains - options after optimisation with fixed budgets

Budget [x £10,000]	Optimal set of options	**Cost of option [x £10,000]**	**Removed Risk [x £10,000]**
7500	1-3,5,20,26,30,38,40-42,44-46, 48-50,53,63-66,68,69,73-75,78,79	7470	59080
9000	1-3,5,20,26,30,38-46, 48-50,53,62-66,68,69,73-75,77-80	9000	65920
11000	1-3,5-6,16,20,26,30,38,40-42,44-46, 48-50,53,60,62-66,68-69,73-75,77-80	11000	74460
12500	1-3,5,6,16,20,26,27,30,38-42,44-46, 48-50,53,60,62-66,68,69,73-75,77-80	12500	80860

8.4.4 Test case 4 – Passenger Door Trap and Drag

To further illustrate the effectiveness of the optimisation tool, it was used for optimising the reduction of a risk that is recurrent in the industry. The results are presented in Table 37.

Let us consider the upgrade of the design of a standard train door following increased incidents of train body-side door trap and drag risks. To reduce the number of incidents in these instances, a number of options are recommended for design improvements. The improved design options aim as far as reasonably practicable, to reduce or eliminate risk of doors trapping passengers (or their clothing, bags etc.) between the doors so that the train pulls off and drags the entrapped passenger. This is a significant risk, which is represented in the fault tree diagram (Figure 61).

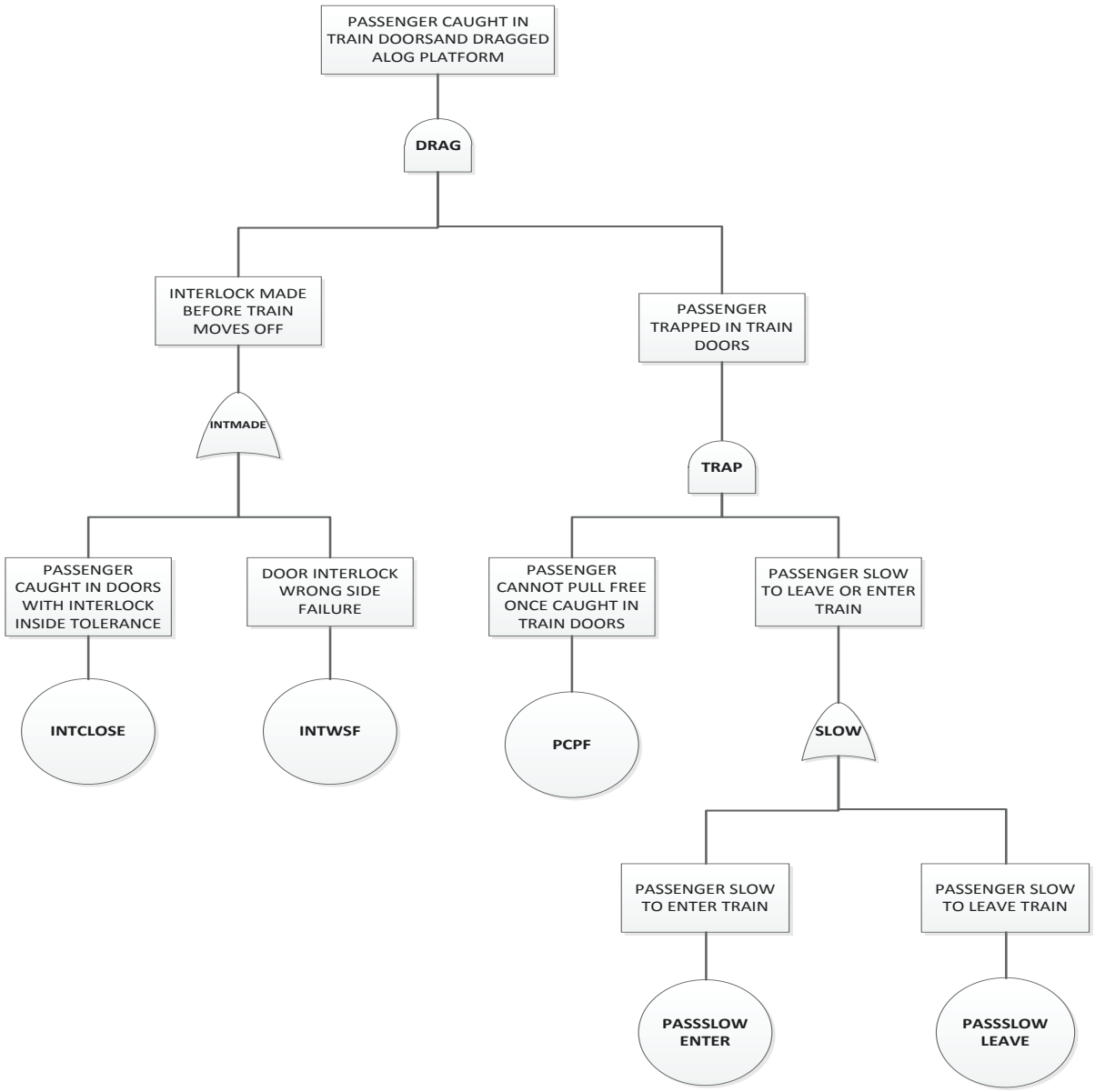


Figure 61: Simplified representation of the typical Train Trap and Drag Fault Tree

Table 35: Train Trap and Drag – Cost and Removed Risk

QRA Event	Event Description
INTCLOSE	Passenger Caught in Doors with Interlock Inside Tolerance
INTWSF	Door Interlock Wrong Side Failure
PCPF	Passenger Cannot Pull Free Once Caught in Train Doors
PASSSLOWENTER	Passenger Slow to Enter Train
PASSSLOWLEAVE	Passenger Slow to Leave Train

In order to reduce the risk of trap and drag, options are recommended which generally conform to standard requirements for body-side doors and include:

- Obstacle detection capability ensuring object detection, the ability to re-open doors to the push back zone of the doors and additional capability to ensure that the door is fully closed;
- Enhanced control of door speed and impact by introducing of locked speed control for the doors across the full stroke of movement. This offers the capability to reduce the impact force to a passenger or an obstruction when closing;
- Anti-dragging features of the door design and condition monitoring of the door, i.e., easy detection and rectification.

The safety benefit was assessed by considering the net change in risk arising from the implementation of the proposed mitigation option. In order to estimate the lifetime risk reduction from the annual risk reduction, the CBA considers the risk reduction to be effective over the life of the system, i.e. 25 years.

Best-fit design and procedural options which could potentially reduce risks associated with the trap and drag event are provided in Appendix A.

A further analysis to assess each option with the aim of determining factors that could possibly influence each option's cost and risk reduction benefit is then undertaken to illustrate the risk reduction benefits following implementation. These are the same standard techniques used in estimating risk benefit and estimated costs during a basic CBA exercise. The assumption is that the risk benefit and estimated costs are known quantities for each option identified.

Table 36: Options for risk reduction with estimated cost benefit

ID	Option for risk reduction	Risk Reduction Benefit	Estimated Cost	Estimated Cost / Benefit
1	Pushback on both door leaves and increase spring forces.	£480,011.00	£491,432.00	1.02
2	Door self-tests on each leaf of each door.	£47,164.00	£44,840.00	0.95
3	No rubber seals: metal-to-metal contact of doors.	£272,608.00	£50,000.00	0.18
4	Dot matrix (PIS) on train exterior to indicate that doors are about to close.	£53,328.00	£5,000.00	0.09
5	Dot matrix (PIS) on train exterior to indicate that doors are about to close.	£53,328.00	£5,000.00	0.09
6	Larger monitor/better resolution.	£13,160.00	£137,240.00	10.43
7	Cameras on the platform to address blind spots	£48,620.00	£42,985.00	0.88
8	Camera on the outside of each car.	£14,476.00	£47,000.00	3.25
9	Slow train acceleration from station	£39,618.00	£140,000.00	3.53
10	Transparent doors	£184,541.00	£1,175,000.00	6.37
11	Pushback on both door leaves.	£7,520.00	£10,456.00	1.39
12	More signs/platform plungers.	£1,681,864.00	£21,000.00	0.01
13	Conductive door edge makes interlock when doors close (two foil edges or carbon seals make circuit).	£464,399.00	£2,000,000.00	4.31

ID	Option for risk reduction	Risk Reduction Benefit	Estimated Cost	Estimated Cost / Benefit
14	On double door, one maglock with magnet placed on one door and reed switch on the other	£287,686.00	£700,000.00	2.43
15	Better signage.	£5,900.00	£12,000.00	2.03
16	Different seal profile - male-to-male profile.	£10,213.00	£60,000.00	5.87
17	Audible announcement (train or platform).	£1,536.00	£3,360.00	2.19
18	Platform CCTV and plunger within the line or station control centre.	£53,333.00	£19,200.00	0.36

Using the 'Trap and Drag' data set, different budgets are applied for achieving the optimal set of risk reduction options and provided in Table 37.

Table 37: Optimal set of risk reduction options (using optimal method)

Budget [x £1,000]	Optimal set of options	Cost of option [x £1,000]	Removed Risk [x £1,000]
250	2,3,4,5,7,8,11,12,17,18	248	2234
280	2,3,4,5,7,8,11,12,15,17,18	260	2240
320	2,3,4,5,7,8,11,12,15,16,17,18	320	2250
350	2,3,4,5,7,9,11,12,15,18	350	2264

8.5 Comparison of the proposed method with the currently adopted strategy in the railway industry.

Any project on the railways – whether greenfield, major renewals or brownfield (maintenance) is constantly subjected to budget constraints. The deficiencies of the widely used cost benefit method for selecting risk reduction options on the railways is comprehensively addressed in Weli and Todinov (2013a). The limitations of this method are clearly illustrated by revisiting Test Case 4 – Trap and Drag (as presented in Section 8.4.4). The application of the dynamic programming technique as introduced by Todinov and Weli (2013), using the same test case, illustrates the effectiveness and superiority of the technique when the objective is optimising risk reduction under fixed budgets.

In order to appropriately compare the optimisation tool and the currently practised cost benefit for selecting options for risk reduction, the simple example of the Door Trap and Drag risk is employed. To simplify the illustration, only 18 risk reduction options are provided to achieve as low as reasonably practicable levels – within a fixed budget (which is today's project reality). The sample size is reasonably small but the illustration shows the effectiveness of this optimisation tool in relatively small applications. The method provides increasingly superior results as the data sets and numbers of possible options expand.

The data in Table 36 is extracted from a major train systems manufacturer, integrator and principal contractor to most of the railways and metros in the world.

This table shows the cost benefit ratio calculations made by the company. All values are approximated to the nearest thousand. This method limits the options possible to a set that provides a cost-benefit of 1 or less. The total cost of implementing the options using the cost benefit method is approximately £188,000 with a risk reduction of £2,210,000. The optimisation tool also achieves a risk reduction of £2,210,000 when provided with a budget of £188,000. This is best result attainable by the cost-benefit's method using this data set.

Given that the cost-benefit looks for options with ratios less than 1, this suggests that those possible are 2, 3, 4, 5, 7, 12 and 18. Any consideration of additional options means option 1 which has a cost-benefit ratio of 1.02 however, over the threshold of 1. Let us consider Option 1, as a case can be made for its cost-benefit value of 1.02. The resultant cost of implementing the Options 1, 2, 3, 4, 5, 7, 12 and 18 significantly increases to £678,000 from £188,000. This is an incredible 260% increase in cost which only achieves a risk reduction of £2,690,000. This is equivalent to a 22% increase in risk reduction and simply illustrates the ineffectiveness of the cost-benefit method and further shows how difficult it is for an optimised risk reduction under budget constraints to be achieved with this method. This clearly demonstrates that if the cost-benefit method is blindly followed (as in cases of this type and other examples provided in previous chapters), no level of budget control during a project can adequately restrain potential cost escalation.

By applying the optimisation method, an existing budget can effectively be used to determine the best options that will provide the most risk reduction. A similar challenge is set and a baseline of options similar to the cost-benefit method is initially selected by the tool, i.e. Options 2, 3, 4, 5, 7, 12 and 18. Budget constraints are incrementally applied and the results provided in Table 37 (see results in Test Case 4, Section 8.4). It is important to note that the optimisation tool works within the constraints of any budget. For this test case, the budget is steadily increased from £188,000 to £200,000. The options selected are 2, 3, 4, 5, 7, 11 and 12, providing a risk reduction of £2,218,000 at a cost of £198,000. Another step increase in budget to £250,000 illustrates a further increase in risk reduction of £2,234,000 at a cost of £248,000, when using Options 2, 3, 4, 5, 7, 8, 11, 12, 17 and 18. The results (also in Table 37 above) reveal that the best options can be selected to support any budget constraints without limiting the options to ratios that are in reality, impracticable.

The budget constraints on the cost-benefit limit the number of options that can be selected from a data set and invariably, the additional risk reduction obtainable. However, using the same data set from the Door Drag and Trap example, the optimisation method achieves an enhanced risk reduction, as illustrated in Table 38. Figure 62 and Figure 63 present the effect of various budget constraints on the methods when applied to Test Case 4. This clearly shows the difference in removed risk between the

proposed optimisation method and existing cost-benefit practice, once budget constraints are applied. This improved risk reduction is a result of the increased number of options that can be considered within the separate budget scenarios that are characteristically neglected by using cost-benefit ratios.

Table 38: Comparison of risk reduction optimisation method against CBA

		Budget Constraints (x £1,000)					
		£188	£200	£250	£280	£320	£350
Achieved Risk Reduction	Cost Benefit	£2,210	£2,210	£2,210	£2,210	£2,210	£2,210
	Optimisation using DP tool	£2,210	£2,218	£2,234	£2,240	£2,250	£2,264

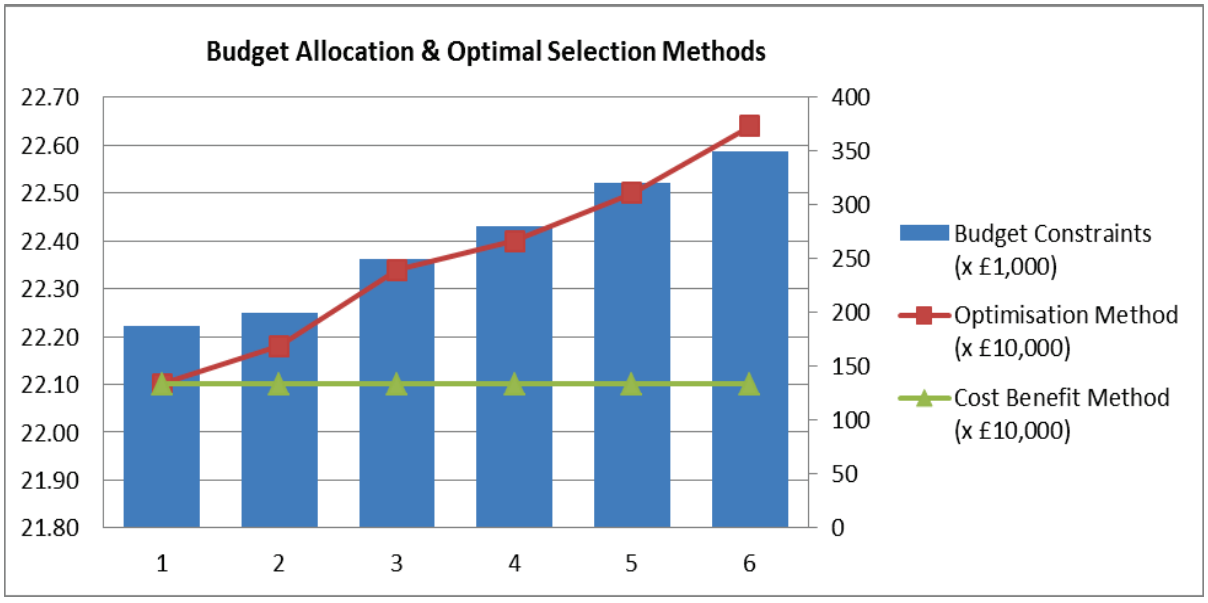


Figure 62: Effect of budget constraints on risk reduction for the option selection methods

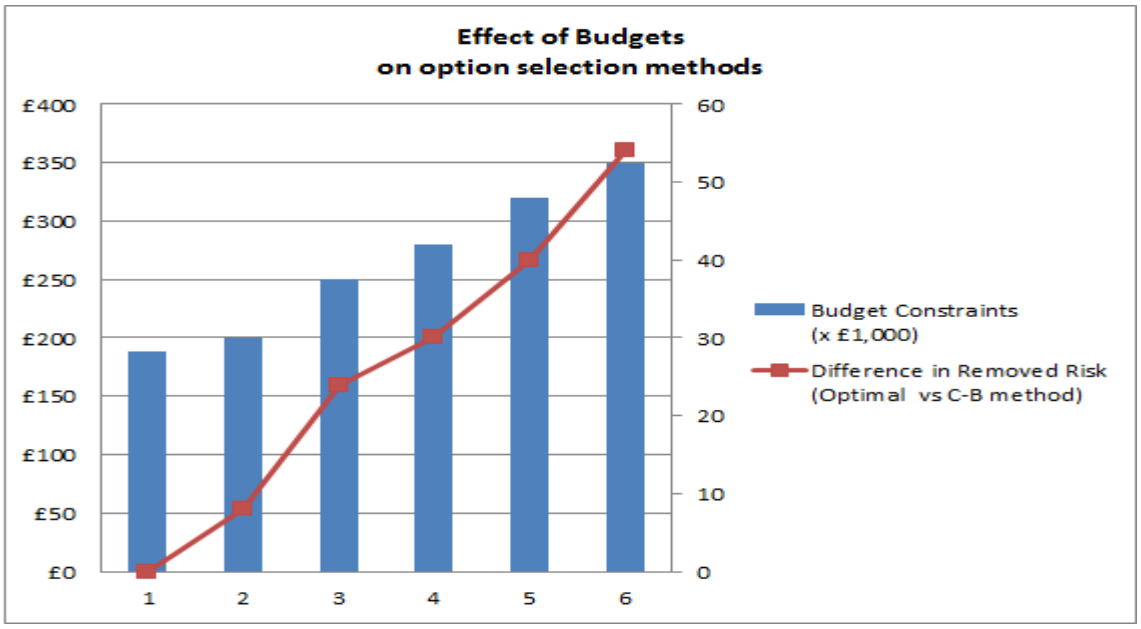


Figure 63: Illustration of the difference in the achievable risk reduction using variable budgets

8.5.1 Advantages of the proposed method

The results reported for real life test cases 1 – 4 prove that the problem related to optimal allocation of a fixed budget to achieve maximum risk reduction in the railway industry can be reduced to an optimisation problem through dynamic programming. The advantages of the latter as an optimisation technique have also been comprehensively addressed.

The objective of this part of the thesis is to develop a platform superior to the existing practices of risk reduction option selection on the railways. As they are mostly based on cost-benefit and other economic theories, such practices have resulted in unfavourable performance, escalating costs, safety risks and business losses for railway operators, facilities owners and the supply chain. The current widely practised methods (particularly cost-benefit methods) for selecting options for risk reduction exposes the decision maker or analyst to uncertain levels of cost and risk.

By using the new concept '**amount of removed risk by a risk reduction option**', the proposed optimisation method solves the problem of a maximum risk reduction resulting in a '*minimised remaining risk*' solution. This is demonstrated to be markedly superior to the current widely used method on the railways, particularly for large test cases.

The advantages of the optimisation method are presented in three main areas – its suitability for meeting regulatory requirements such as the ALARP framework, its effective reduction of assessment errors, i.e. its suitability as comprehensive decision support tool, and its efficiency in terms of computation time.

The ALARP framework stipulates that a comprehensive evaluation of all possible options for risk reduction and a subsequent value-driven decision must be made. In practice, the demonstration of ALARP requires that the sacrifice of introducing further risk reduction measures should not be 'grossly disproportionate' to the benefit that is obtained from the introduction of such measures. Based on the ALARP requirements, different organisations would conventionally apply mandatory steps for illustrating and proving that risk is reduced to ALARP.

The method set out above comprehensively achieves the requirements of the ALARP framework. Following a comprehensive hazard identification and derivation of risk reduction options, the proposed optimisation method seeks out all available options with a potential amount of removed risk and associated costs. Based on the objective function value, it derives the best set within economic constraints (budget).

The use of an industry agreed factor to show that the cost is not grossly disproportionate to the benefit of a particular risk reduction option is, in most capital programmes, used as the budget. Considering the several different subsystems, processes and combinations of measures that are required within this budget constraint, the proposed optimisation method is an effective solution to the challenge posed by the allocation of a limited budget.

This is also particularly necessary in the current economic downturn, with budget cuts to essential projects. The recent government budgetary reviews have dramatically reduced funding for priority projects such as renewals on mainline and underground railway systems and projects. The current theme is 'maintaining risk levels'. With the reality of such cuts putting managers under intense pressure, the method described goes a long way to maximise risk reduction under specified budgets and is an excellent tool countering the impact of the growing austerity measures currently affecting the railways.

The widely used CBA in railway applications does not incorporate all the factors (and certainly not all risk reduction options) that influence engineering judgements on the right choice of system to implement. To remove doubt, Section 8.5 demonstrates that cost-benefit methods are ineffective when budget constraints are applied. Cost-benefit methods totally neglect the marginal benefit to be derived from a complete set of options.

By using the proposed optimisation method, all available options are considered during the computation process, thus reducing the unavoidable build-up of uncertainties inherent in risk assessments made before the option selection process.

Furthermore, **the 'curse of dimensionality' as described in Section 7.7 has been shown to have no effect on this optimisation method**. It is very efficient for solving optimal risk reduction problems with computation time ranging from less than 0.01 seconds for small- and medium-sized data sets (i.e. 10 to 50 options) to 0.15 seconds for large-scale data (i.e. over 80 options) with varying magnitudes of risk reduction and associated costs.

8.5.2 Disadvantages of the proposed method.

For an overall risk management objective, the effectiveness of the optimisation method is dependent on a comprehensive risk assessment process and subsequently, options for risk reduction. Weli and Todinov (2013a) propose a sound and verifiable approach, based on structured engineering principles, from which risk reduction options are identified. The application of this method before optimisation reduces the inherent weaknesses of risk identification and assessment such as uncertainties in data, errors in judgements concerning risks, among others.

The proposed optimisation method is limited to independent risk reduction options. Interactions between subsystems – an essential factor for effective risk reduction are not easily modelled. The optimisation method however, produces an exact solution for all computations.

Examples of these essential interactions are provided in Section 7.3. Weli and Todinov (2013b) present a systems approach to risk reduction that shows the interconnectivity between subsystems, systems and application. The paper also illustrates how risk reduction can be improved through this link and effectiveness from initiation (analysis) to implementation (organisation).

8.6 Validation of the proposed method

In the absence of real-life verifiable railways optimisation applications with known practical solutions, validation is demonstrated through comparison of the test results with mathematical solutions from resource allocation examples downloaded from the internet. The data sets used for validation are taken from various optimisation (dynamic programming or knapsack) exercises from different applications and industries.

The examples have been extracted from real optimisation cases for which the solution is known. The knapsack validation exercises are further proof that the proposed algorithm is successful when the options are statistically independent and gives an exact solution for each test. Validation using data set 1 is presented in Table 39 below:

Table 39: Validation - Data Set-1

ID	Risk Reduction Benefit	Estimated Cost
1	92	23
2	57	31
3	49	29
4	68	44
5	60	53
6	43	38
7	67	63
8	84	85
9	87	89
10	72	82

With a budget value of 165, the optimal solution includes Options 1, 2, 3, 4 and 6. The options are accurate to the known optimisation results from the example used.

Validation checks using data set 2 are presented in Table 40

Table 40: Validation - Data Set-2

ID	Risk Reduction Benefit	Estimated Cost
1	135	70
2	139	73
3	149	77
4	150	80
5	156	82
6	163	87
7	173	90
8	184	94
9	192	98
10	201	106
11	210	110
12	214	113
13	221	115
14	229	118
15	240	120

A budget value of 750 imposed on the set of 15 options provided the following options as optimal: 1, 3, 5, 7, 8, 9, 14, and 15. An evaluation against the known solution shows another accurate solution using the proposed algorithm. Similarly, the algorithm was tested using the data set presented in Table 41.

Table 41: Validation - Data Set-3

ID	Risk Reduction Benefit	Estimated Cost
1	825594	382745
2	1677009	799601
3	1676628	909247
4	1523970	729069
5	943972	467902
6	97426	44328
7	69666	34610
8	1296457	698150
9	1679693	823460

ID	Risk Reduction Benefit	Estimated Cost
10	1902996	903959
11	1844992	853665
12	1049289	551830
13	1252836	610856
14	1319836	670702
15	953277	488960
16	2067538	951111
17	675367	323046
18	853655	446298
19	1826027	931161
20	65731	31385
21	901489	496951
22	577243	264724
23	466257	224916
24	369261	169684

A budget value constraint of 6404180 is used on the set of 24 options provided in Table 41. The accurate optimal solution includes 1, 2, 4, 5, 6, 10, 11, 13, 16, 22, 23, and 24. This result further verified the accuracy of the optimisation algorithm.

The experimental results demonstrate that the proposed algorithm producing always the exact solution can accurately support any decisions associated with optimising risk reduction within a fixed budget.

8.7 Case for implementing the optimisation method to support efficient decision making and risk

The economic resources available for capital programmes, maintenance and interventions are usually limited: thus the need arises for optimally allocating them to achieve the best possible risk reduction.

This chapter focused on presenting a novel algorithmic method for targeting the allocation of budgets to options with sufficient value in order to minimise the overall system and operational risks. The optimisation of risk reduction options concerns the stages of decision analysis, where exact solutions from algorithms and models are required to support decisions to invest in systems that achieve the target of maximum risk reduction under budget constraints. To reduce the flaws in the overall objective a more inclusive 'best options-search' has been introduced to improve risk-based decisions in the railway industry.

In developing this algorithm, important factors considered were the regulatory policies, such as the ALARP framework. This is usually a basis for budget constraints, probabilistic quantification of risk or risk exposures, cost of equipment and systems, risk reducing options and resource allocation. The model has been cautiously constructed to avoid unquantifiable units i.e. things without a price tag.

To the pure economist, the value of the tangible and intangible depends on the price a person is willing to pay for an object. In this method, developed solely for efficiently optimising risk reduction within a fixed budget, Willingness-to-Pay and the Value of Preventing Fatality are taken as parameters determined outside the scope of the optimisation model.

The decision support optimisation algorithm was computed using 3 different processors to demonstrate accuracy and consistency of results and computation time:

- Intel(R) Core(TM) 2 Duo CPU T9900 @ 3.06 GHz
- Intel(R) Core(TM) i3 CPU M370 @2.40 GHz
- Intel(R) Core(TM) i5 CPU M540 @2.53GHz

In all cases, using the same parameters of risk removed, cost and budget, each of the optimisation problems produced the same results with a maximum computation time of 0.15secs for the largest data set. A degree of uncertainty in the approach used to estimate probabilities and the frequency of risk events during quantified risk assessments is already assumed.

Most railway network projects or undertakings will not always have cases where the risk reduction benefit outweighs the cost (i.e. cost effective risk reduction). In addition the inherent inaccuracies in risk evaluations before selection of the options further obscure any argument of rationality or effectiveness.

In practice, we are often faced with a good number of options where the costs outweigh the safety benefit. What do we do then? Do we ignore viable options because of cost implications and in so doing expose the system and passenger to further risks?

Is it justifiable to use the existing approach when it is obviously fundamentally flawed? The novel approach presented here considers the maximum risk reduction within a fixed budget by factoring in all relevant risk reduction options irrespective of individual costs (which are subject to errors in individual assigned risk reduction values).

In practical terms, let us assume that no cheaper option exists for a given scenario. Nonetheless, the safety risk has to be minimised (to ALARP) within specified overall budget constraints. Using a signalling overlap example, the installation or introduction of speed restrictions may only marginally reduce the risk but still leave it within the ALARP range where further risk reduction is necessary. Despite the existence of 'non-conforming cost-benefit' options such as an overlap extension that could potentially be added to the speed restriction, those options are discounted. The question remains – have we done everything possible to ensure maximum risk reduction within the specified budget?

With the existing methodology, the answer is '*No.'* As a result, potentially viable options are left out of most railway industry selection methods.

The processes, activities or prerequisites of the maximum risk reduction approach presented in this chapter can be summarised as:

- Application of robust processes or methods for identifying risks and contributors

- Application of sound and verifiable means of evaluating the magnitude of risks reduced by the options identified
- Application of a comprehensive method for deriving the cost of each risk-reduction option

Chapter 9 Conclusions, Contributions and Future Work

The core objectives of this work, - developing a novel solution for the problem of optimising risk reduction within a fixed budget, which is systematic, verifiable and fitting for the railway industry in the current economic climate, has been achieved. In this respect, the most important findings and contributions of this research are highlighted.

- This thesis has established that the ***cost-benefit approach fails to determine the optimal selection of options leading to a maximum risk reduction when a budget limitation is present***.
- The thesis has shown that only ***verifiable methods based on sound engineering principles can objectively result in optimum risk reduction***.
- The thesis pioneered **the application of powerful dynamic programming model for effective risk reduction in the railway industry.**
- This thesis reveals *the* ***critical deficiency of the maximum expected profit criterion in selecting a risk reduction option.***
- The ***tools currently being used for optimising risk reduction are ineffective***. In addition, these ***tools cannot be modified to solve the maximum risk reduction problem when budget constraints are applied***.
- ***Guidelines and systematically developed methods for precisely identifying and applying known measures to reduce the likelihood of accidents or the consequences in the event of the accidents are non-existent***. This is the corner stone to any risk optimisation effort.
- This thesis established that the ***challenge of optimal risk reduction cannot be solved by the preventive-first approach (i.e. selecting options primarily for reducing the likelihood of the accident only)*** as widely practiced. This approach leads to weak and potentially damaging decisions. This thesis proves through practical illustrations and by the use of mathematical methods that ***the choice of risk reduction measures to achieve the maximum effect is significantly influenced by the available budget and how the contributors to accidents are targeted and managed***.
- With the aid of practical railway illustrations, this thesis demonstrates that a severe defect in existing methods for selecting measures is ***the lack of structured methods for comprehensively identifying all interactions that support the maximum risk reduction***. By revealing the complex interrelationships between the risk reduction options; the gap between risk evaluation, options

selection and implementation can be effectively narrowed. Subsequently, the weakness in the risk management chain (i.e. costs, people, process and equipment) can effectively be eliminated.

- The thesis demonstrated that in the current risk management practice, ***the link between the evaluation and implementation phases of risk-reduction is commonly overlooked or disregarded***. As a result, this erroneous practice is a significant bottle-neck in gaining approval of submissions for operational safety (risk reduction).

Considering the above, this project has gone beyond the basic case of cost effective risk management to propose concepts and verifiable methods that can be considered for optimising risk reduction when faced with budget constraints – the growing reality of the railway industry. These concepts and methods have been applied to specific examples with known solutions in which realistic and exact numerical values are achieved. This work is novel and the first to deliver on a robust decision support framework that comprehensively supports a railway operational case for maximising risk reduction when faced with fixed budgets. The flow diagram (Figure 64) clarifies the primary contributions and how they are applicable to the overall objective of this thesis.

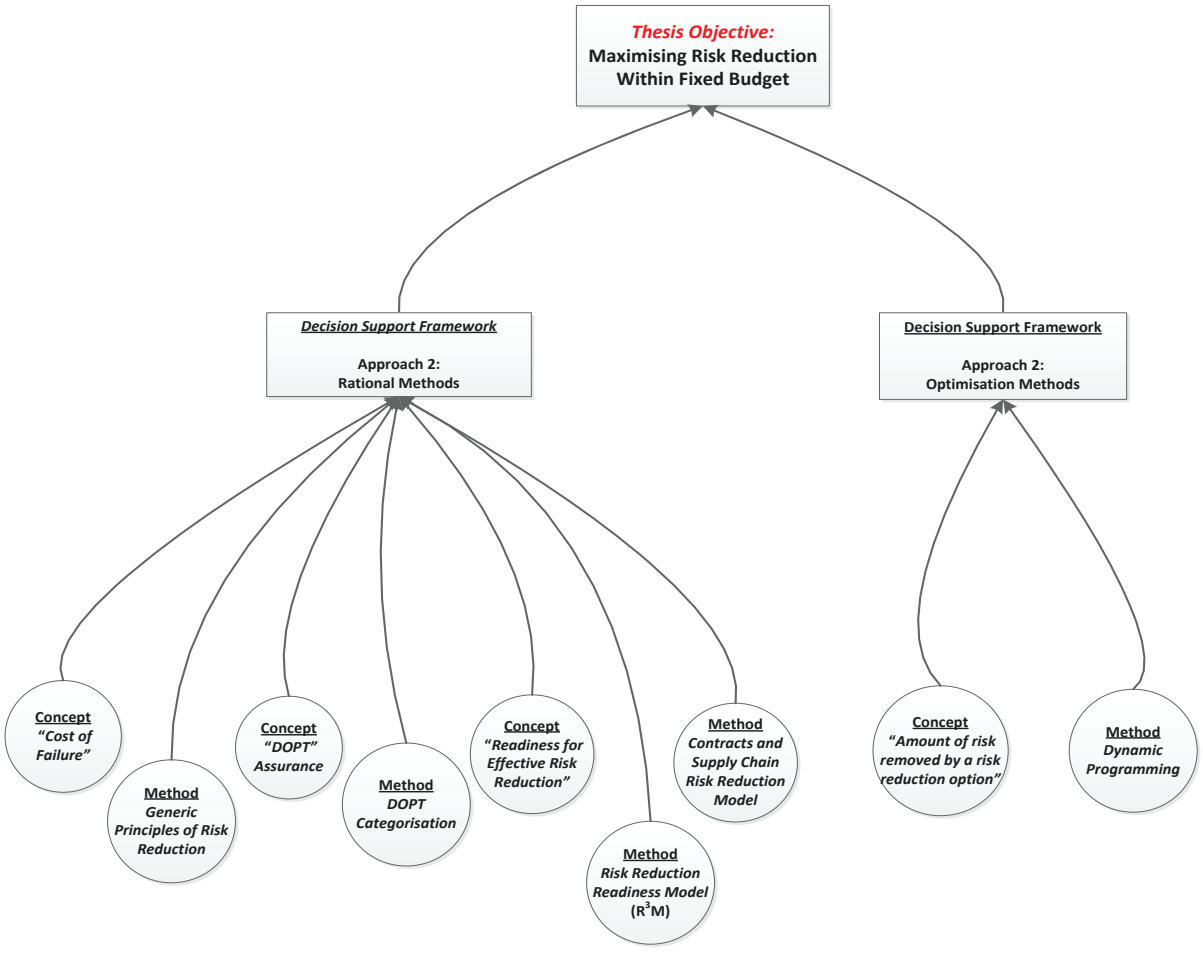


Figure 64: Thesis objective and achievements

- ***Cost of Failure' concept and generic principles of risk reduction***

  By using the 'cost-of-failure' (CoF) concept and the generic principles of risk reduction, an appropriate set of generic risk-reduction principles has been developed, specific to the railway industry, from which risk-reduction measures are derived (Chapters, 5, 6 and 7). These measures reduce the likelihood of a railway accident or the consequences in the event of an accident. Subsequently, the identified risk-reduction measures are assessed with regards to the amount of risk each of them removes and the cost of their implementation.

- ***Application of risk reduction principles on the railway network***

  A comprehensive understanding of the limitations and strengths of each option for the specific application is a prerequisite for effective overall risk reduction. Using the principles in Chapters 5 and 6, railway applications of risk reduction measures are comprehensively outlined providing the risk analyst or decision maker an authentic baseline for selecting and combining measures for prevention or protection. A significant step towards the overall optimisation goal and easily verifiable when developing a robust engineering or operational (risk reduction) safety case.

- ***Classification and guidance for risk reduction measures***

  Considering that no form of guidance or verifiable system exists to help railway risk analysts and decision-makers determine what part a risk reduction option plays in any specific application, this work uses the basic principles of risk reduction to classify options as preventive or protective. The thesis employs 26 fundamental principles to develop an extensive yet simple classification based on the options of functional capability (strengths and limitations) for the particular application.

  This clear and unambiguous method for determining whether an option is appropriate for use as a preventive or protective measure provides the risk analyst with a degree of confidence that the selected option stems from fundamental risk reduction principles. A comprehensive list with classification based on the work in Chapters 5 and 6 is provided in Appendices A1, A2 and A3 for the major accident risks 'Collision Between Trains', 'Derailment' and 'Platform Train Incidents' respectively.

- ***Concept and Application of 'D-O-P-T Assurance'***

  Based on a sound argument that by integrating the initiation (evaluation) phase with the implementation (operational) phase of a project, cost-effective risk management can be achieved, this work introduces a key assurance concept and methodology that categorises risk reduction measures for a standard railway portfolio. The DOPT categorisation approach reflects the options and organisation, providing the necessary link that ensures an option can be

accurately and systematically identified and subsequently implemented. The categorisation (see Chapter 7) includes:

- *Design risk-reduction options (DRRO)* – Novel systems, major renewals and modifications
- *Operational risk-reduction options (ORRO)* – Communications, Supervision and Speed Restrictions or similar operational decisions
- *Technical risk-reduction options (TRRO)* – Testing, Maintenance, Inspections, Installations, Assessments/Studies informing risk reduction decisions
- *Procedural risk-reduction options (PRRO)* – Risk education, Risk training, Processes and Plans

This concept provides a novel framework that bridges the divide between the identification and implementation of risk reduction measures within railway organisations.

- ***Concept of 'Readiness for Effective Risk Reduction' and the Risk Reduction Readiness Model (R^3M).***

  This work is based on the foundations of system engineering, and uses the systems approach to demonstrate the inter-relationship between risk reduction evaluation and implementation. The concept of 'Readiness for Effective Risk Reduction' is developed and recommended as a required and fundamental process in railway safety cases. An essential framework is presented in the form of the 'Risk Reduction Readiness Models' (R^3M).

- ***Contracts and Supply Chain Risk Reduction Model***

  Due to the vital role played by procurement and contracts in assuring that risk reduction requirements are captured and executed, a simplified model, aligned with the essence of the concept of 'Readiness for Effective Risk Reduction' is developed. It provides a solution to the major challenges facing railway contracts and procurement i.e. frequent failure partnerships and lack of robust systems for product recalls associated with safety related failures.

- ***Optimisation Model***

  Finally, the concept of *'amount of risk removed by a risk reduction option'* is introduced as a superior alternative to the widely used cost-benefit method.

  This novel approach resulted in the development of a robust tool that provides exact optimal solutions for a relatively large number of options. The computation is also achieved within a relatively short time, making the developed system an efficient decision support tool for the

railway industry. Chapter 8 presents the method, algorithms, and four test cases using railway safety risk data. Validation exercises were also conducted and results presented.

It is worth noting that as a consequence of elements of this work, an invitation to join the editorial board of the Journal of Geological Resource and Engineering was received. A clear indication of acceptance of the concepts and methods proposed. Additionally, this demonstrates the potential application of these concepts and methods in a different application (i.e. geotechnical and petroleum technology industry)..

9.1 Overall Summary

This work demonstrates that the current conventional methods for selecting risk reduction measures is limited in its ability to adequately support the overall risk management objective of maximising risk reduction within fixed budgets. In fact, the practice leads to misleading results and incorrect risk reduction-related decisions.

A comprehensive understanding of the limitations and strengths of each option for the specific application is successfully applied for effective overall risk reduction. Applications from decisions based on the successful integration and implementation of the available options are demonstrated as superior to existing methods and shown as a powerful tool for solving current decision-making challenges on optimising risk reduction.

The methods proposed substantially reduce and remove the inadequacies of the methods currently practised. Currently, optimisation techniques to the problem of risk reduction and budget allocation are not being practised on the railways due to the dominance of cost-benefit methods. By the use of verifiable concepts and methods, this thesis offers a framework combining a rational approach with exact optimisation techniques. This has been demonstrated by the much more precise solutions from the proposed optimisation tool.

The suggested framework is a holistic approach to maximising risk reduction within specified budget constraints and a robust solution to the growing complexities associated with operating the current railway network.

The relevance of the solutions provided by this framework stems from the common shortage of funds for railway projects. Recent economic downturns with ongoing significant cuts affect maintenance and capital projects and expose railway operators, staff, passengers and others to the consequences of performance and safety risks. Despite these cuts, the proposed optimisation techniques guarantee that the safety expectations and the level of control of consequences in the event of failure will not be degraded.

The framework for maximising risk reduction within specified budgets has proved advantageous as it further increases safety assurance - potentially amounting to significant magnitudes of reduced risk. This thesis concludes that increased cost effectiveness can be derived from the combination of the rational risk reduction strategies and the optimal budget allocation techniques..

9.2 Future Work

The presented concepts and methods can be readily extended to other industries where the widespread practices of cost-benefit and various economic theories are delivering sub-optimal solutions, misrepresenting and underachieving risk reduction. The aim is to unify the approaches and develop a framework that pushes further into an organisation's core risk management structures.

In order to support the existing framework, a method needs to be developed to introduce cross acceptance of risks and responsibilities within the organisation (i.e., between the different departments), allying the strengths and limitations of the options to the existing systems of risk management within the existing departments.

An optimisation tool could be devised that is capable of analysing not only relatively independent risk reduction options but could consider various complex interactions (within the subsystems, systems in an organisation) from initiation through to implementation. The difficulties of modelling different states stems from the circumstance that the state-space could grow exponentially in larger models, reducing the feasibility of the approach.

It is recommended that the DOPT Assurance Case is enhanced and made a mandatory requirement for developing robust safety cases in the railway industry and other related safety-critical industries.

As a result of the comprehensive evaluations and current system opportunities highlighted through this work, new process and assessment requirements need to be examined in order to determine the railway organisation's maturity levels for risk reduction throughout any project lifecycle. Recommendations include extension of the work on the risk reduction readiness models i.e. beyond contracts and procurement.

REFERENCES

Adler, M.D., Posner, E.A. (2000). Cost Benefit Analysis – Legal, Economic and Philosophical Perspectives. The University of Chicago Press, Ltd.

Ahonena, J.J., Savolainena, P. (2010). Software engineering projects may fail before they are started: Post-mortem analysis of five cancelled projects. The Journal of Systems and Software, 83: 2175–2187.

Allais, M. (1953). Le comportement de l'homme rationnel devant le risque: critique des postulats et axiomes de l'école Américaine. Econometrica, 21: 503-546.

Alvarez, F., Stokey, N.L. (1998). Dynamic Programming with Homogeneous Functions. Journal of Economic Theory, 82: 167-89

An, M., Chen, Y., Baker, C.J. (2011). A fuzzy reasoning and fuzzy analytical hierarchy process based approach to the process of railway risk information: A railway risk management system. Information Sciences 181: 3946–3966.

Arkes, H.R. (1991). The costs and benefits of judgement errors: Implications of debiasing. Psychology Bulletin, 110: 48-498

Arrow, K. J., Lind, R. C. (1970). Uncertainty and the Evaluation of Public Investment Decisions.American Economic Review, 60: 364-378.

Arunkumara, S. (1975). Characterization of Optimal Operating Policies for Finite Dams. Journal of Mathematical Analysis and Applications, 49: 267-274.

Aven, T., Vinnem, J.E., Vollen, F. (2006). Perspectives on Risk Acceptance Criteria and Management for Offshore Applications – Application to a Development Project. International Journal of Materials & Structural Reliability 4 (1): 15-25.

Aven, T., Kørte, J. (2003). On the use of risk and decision analysis to support decision-making. Reliability Engineering and System Safety, 79: 289–299.

Baccarini, D. (1996). The concept of project complexity - a review. International Journal of Project Management, 14: 201-4

Baker, N.R., Sweeney, D.J. (1978). Toward a conceptual framework of the process of organized innovation technological within the firm. Research Policy, 7: 150-174.

Baker, R. (1980). Determination of the critical slip surface in slope stability computations. International Journal for Numerical and Analytical Methods in Geomechanics, 4: 333-59

Ball, D.J., Floyd, P.J. (1998). Societal Risks - Final Report to HSE. Sudbury, Suffolk: HSE Books.

Balas, E., Zemel E. (1980). An Algorithm for Large Zero-One Knapsack Problems. Operations Research, 28: 1130–1154.

Basso, A., Peccati, L.A. (2001). Optimal resource allocation with minimum activation levels and fixed costs – Theory and methodology. European Journal of Operational Research, 131: 536-549

Baysari, M. T., McIntosh, A. S., Wilson, J. R. (2008). Understanding the human factors contribution to railway accidents and incidents in Australia. Accident Analysis and Prevention, 40: 1750–1757.

Beale, C. J. (2002). Recent Railway Industry Accidents - Learning Points for the Process Industries. Institution of Chemical Engineers. Process Safety and Environmental Protection, 80 (1): 25 – 32.

Beattie, J., et al (1998). On the Contingent Valuation of Safety and the Safety of Contingent Valuation: Part 1-Caveat Investigator. Journal of Risk and Uncertainty, 17: 5–25

Bellman, R. (1957). Dynamic programming. Princeton, N. J., Princeton University Press

Bellman, R., Dreyfus, S. (1959). Functional approximations and dynamic programming, Mathematic Tables and Other Aids to Computation, 13 (68): 247-251.

Bellman, R., Dreyfus, S. (1962). Applied Dynamic Programming. Princeton, NJ: Princeton University Press.

Bemment, S., Dixon, R., Goodall, RM and Brown, S. (2013). Redundantly Engineered Track Switching for Enhanced Railway Nodal Capacity, Proc 1st IFAC ACATTA Workshop, Istanbul.

Bessant, J. (1991). Managing Advanced Manufacturing Technology: The Challenge of the Fifth Wave. Manchester: NCC- Blackwell.

Bessis, J. (2002). Risk Management in Banking. Hoboken NJ: John Wiley & Sons, 2nd Edition.

Bhardwaj, A., Tung, N.S., Kamboj, V. (2012). Unit Commitment in Power System: A Review. International Journal of Electrical and Power Engineering, 6(1): 51 – 57.

Bhattacharjee, D. (2007). A Proposed Cost-benefit Analysis Model for Physical Form Analysis for a Futuristic Submarine Decision Support System. Master's Thesis, Cambridge: Massachusetts Institute of Technology

Bjorndal, M.H. Caprara, A., Cowling, P.I., Croce, F.D., Lourenco, H., Malucelli, F., Orman, A. J., Pisinger, D., Rego, C., Salazar, J. J. (1995). Some thoughts on combinatorial optimization. European Journal of Operational Research, 83: 253-270

Blackorby C., Donaldson, D. (1990). A review article: The case against the use of the sum of compensating variations in cost-benefit analysis. Canadian Journal of Economics, 23: 471-94.

Boardman, A.E., Greenberg, D.H., Vining, A.R., Weimer, D.L. (2006). Cost Benefit Analysis – Concepts and Practice. Oxford: Prentice Hall, 3rd edn.

Borysiewicz, M.J., Borysiewicz, M.A., Garanty, I., Kozubal A. (2004). Models and techniques for Health and Environment Hazard Assessment and Management. IAEA Report on Quantitative Risk Assessment (QRA). CoE MANHAZ, Institute of Atomic Energy, 111-127: 300-309).

Brent, R.J. (2006). Applied Cost Benefit Analysis. Cheltenham: Edward Edgar Publishing Ltd, 2nd edn.

Brzozowska, K. (2007). Cost-Benefit Analysis in Public Project Appraisal. Engineering Economics, 3 (53): 78-83

Busby J.S. (2008). Analysing Complicity in Risk. Risk Analysis, 28 (6): 1571-82

Busby, J.S. (1998). The neglect of feedback in engineering design organisations. Design Studies, 19: 103-117

Busby, J.S., Hebbard, R.E. (2004). Artefacts, Sense-making and Catastrophic Failure in Railway Systems. Paper presented at the IEE International Conference on Systems, Man and Cybernetics, 6198- 6205.

Cagno E., Di Giulio, A., Trucco, P. (2001). An algorithm for the implementation of safety improvement programs. Safety Science, 37: 59-75.

Cai, C., Wong, C.K., Heydecker, B.G., (2009). Adaptive traffic signal control using approximate dynamic programming. Transportation Research Part C: Emerging Technologies, 17(5): 456-474.

Camerer, C. F., Kunreuther, H. (1989). Decision Processes for Low Probability Events: Policy Implications. Journal of Policy Analysis and Management, 8 (4): 565-92

Campbell, H., Brown, R. (2003). Benefit-Cost Analysis: Financial and Economic Appraisal Using Spreadsheets. Cambridge: Cambridge University Press.

Caputo, A.C., Pelagagge, P.M., Palumbo, M. (2011). Economic optimization of industrial safety measures using genetic algorithms. Journal of Loss Prevention in the Process Industries, 24: 541-551

Carlile, P. R. (2002). A pragmatic view of knowledge and boundaries: Boundary objects in new product development. Organ. Sci. 13 (4): 442-55

Chai, C., Wong, C.K., Heydecker, B.G. (2009). Adaptive traffic signal control using approximate dynamic programming. Transportation Research Part C, 17(5): 456-74

Chakraborty, A. (2009). Fault Tolerant Fail Safe System for Railway Signalling. Proceedings of the World Congress on Engineering and Computer Science, 2. San Francisco, USA.

Chao, L., Hsiao C. (2012). Fuzzy model for predicting project performance based on procurement experiences. Automation in Construction, 28: 71-81.

Chapman, L.., Thornes, J.E., Huang, Y., Sanderson, V.L., Cai, X., White, S.P (2008). Modelling of rail surface temperatures. Theoretical and Applied Meteorology, 92:121-131

Considine, M. (1984). The Assessment of Individual and Societal Risks. SRD Report R-310, Safety and Reliability Directorate. Warrington: UK Atomic Energy Authority

Contractor, N. S., Monge, P. R. (2002). Managing knowledge net-works. Management Communication. Quarterly. 16(2): 249-58

Cooper, D.F., Grey, S., Raymond, G., Walker, P. (2005). Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements. Hoboken NJ: John Wiley & Sons

Corbett, L.M., Brockelsby, J., Campbell-Hunt, C. (2002). Tackling industrial complexity. Cambridge: Institute for Manufacturing

CRI (2005). Britain's Railway Crisis – A review of the arguments in comparative perspective. University of Bath Centre for the Study of Regulated Industries: Occasional Paper 20

Cullen, A.C., Frey, H.C. (1999). Probabilistic techniques in exposure assessment. A handbook for dealing with variability and uncertainty in models and inputs, New York: Plenum

Currie, D. (2000). 'Funding the London Underground', London Business School, Regulation DETR Press Notice 213. London Underground Ltd

Davies, D.E.N. (2000). Automatic Train Protection for the railway network in Britain - a study. Royal Academy of Engineering, London.

Dasgputa, A.K., Pearce, D.W. (1972). Cost Benefit Analysis – Theory and Practice, London: The Macmillan Press Ltd.

Dasgupta, S., Papadimitriou, C., Vazirani, U. (2008). Algorithms. McGraw Hill, Boston, 2008

de Felice, F., Petrillo, A. (2011). Methodological Approach for Performing Human Reliability and Error Analysis in Railway Transportation System. International Journal of Engineering and Technology, 3 (5): 341-353

de Finetti, B. [1937]. 'Foresight: it's Logical Laws, its Subjective Sources' in Kyburg, H. E., Smokler, H. E. (eds), Studies in Subjective Probability. Hoboken NJ: Wiley (English trans.)

Dft (2008). Transport Statistics Great Britain 2008, 34th edn

Dft (2010). Transport Statistics Great Britain - 2010. Transport Accidents and Casualties. Department for Transport – National Statistics: http://www.dft.gov.uk/pgr/statistics/datatablespublications/tsgb/latest/tsgb2010accidents.pdf. Accessed 03-04-2011

Dft (2013). The Department for Transport's Transport Analysis Guidance: The Estimation and Treatment of Scheme Costs (September 2006), (TAG) Unit 3.5.9.

DNV Technica (1999). "A Guide To Quantitative Risk Assessment for Offshore Installations". DNV Technica Publication, 99/100a: 176-185

Dobney, K., Baker, C.J., Chapman, L., Quinn, A.D. (2010). The future cost to the UK's railway network of heat related delays and buckles caused by the predicted increase in high summer temperatures due to climate change. Proceedings of the Institution of Mechanical Engineers, Part F, Journal of Rail and Rapid Transit 224:25-34.

Druschel, P., Abbot, M.B., Pagels, M.A., Peterson, L.L (1993). Network Subsystem Design. IEEE Network, 7(4):8.

Dumus, M.S., Eris, O., Yildirim, U., Soylemex, M.T. (2011). A new voting strategy in diverse programming for railway interlocking systems. International Conference on Transportation, Mechanical and Electrical Engineering, 723 – 726.

Ebrecht, L., Horste, M.M. (2012). Verification and Validation of Interoperability. Published in "Railway safety, reliability and security: technologies and systems engineering". IGI Global, Pennsylvania.

Eddy, S. R. (2004). 'What is dynamic programming?' Nature Biotechnology, 22: 7, 909-10

Elhorst, J.P., Oosterhaven, J. (2008). Integral cost-benefit analysis of Maglev projects under market imperfections. Journal of Transport and Land Use, 1(1): 65-87

Ellsberg, D. (1961). Risk, Ambiguity, and the Savage Axioms, Quarterly Journal of Economics, 75(4): 643-69

Elvik, R. (2001). Cost–benefit analysis of road safety measures: applicability and controversies. Accident Analysis and Prevention, 33: 9–17.

Eriksen, K.S., Jensen, S. (2010). The cost of second best pricing and the value of risk premium. Research in Transportation Economics, 30:29-37.

Evans, A.W., (1996). The Economics of Automatic Train Protection in Britain, Transport Policy, 3:105-110

Evans A.W., Verlander, N. (1997). What is wrong with criterion FN-lines for judging the tolerability of risk? Risk Analysis, 17(2): 157-68.

Evans, A.W. (2003). Estimating transport fatality risk from past accident data. Accident Analysis and Prevention, 35: 459-72.

Evans, A.W. (2005). Proceedings of the Institution of Civil Engineers. Transport 158, 13852 (TR1): 3 – 9.

Evans, A.W. (2007). Rail safety and rail privatisation in Britain. Accident Analysis and Prevention, 39 (3): 510–523.

European Railway Safety Directive (2004/49) amended by Directive 2008/57/EC and Directive 2008/110/EC. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0062:0067:EN:PDF. Accessed 07-07-13.

Fang, C., Marle, F., Zio, E., Bocquet, J. (2012). Network theory-based analysis of risk interactions in large engineering projects. Reliability Engineering and System Safety, 106: 1-10

Fenelon P., McDermid, J.A. (1993). An integrated toolset for software safety analysis. Journal of Systems and Software 21(3): 279-90

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L. & Keeney, R. L. (1981). Acceptable Risk. New York: Cambridge University Press

Flyvbjerg, B., Holm, M.S., Buhl, S. (2002). 'Underestimating Costs in Public Works Projects Error or Lie?' Journal of the American Planning Association, 68 (3): 279-95

Flyvbjerg, B., Holm, M., Skamris, K., Buhl, S.L. (2003). How common and how large are Cost Overruns in Transport Infrastructure Projects? Transport Reviews, 23 (1): 71-88

Fukuba, Y., Ito, K. (1984). "The so-called expected utility theory is inadequate". Mathematical Social Sciences, 7: 1-12

Gaur, D. (2005). Human factors analysis and classification system applied to civil aircraft accidents in India. Aviation, Space, and Environmental Medicine, 76 (5): 501–505.

Ghazinoory, S., Aliahmadi A., Namdarzangeneh, S., Ghodsypour, S.H. (2007). "Using AHP and L.P. for choosing the best alternatives based the gap analysis". Applied Mathematics and Computation, 184: 316–321.

Ge, X., Paige, R.F., McDermid, J.A. (2009). Probabilistic failure propagation and transformation analysis. Computer Safety, Reliability and, Security, 5775: 215-28

Gessford, J., Karlin, S. (1958). 'Optimal Policy for Hydroelectric Operations, Studies in the Theory of Inventory and Production' in K.J. Arrow, S. Karlin and H. Scarf (eds.), Studies in the Mathematical Theory of Inventory and Production, Stanford Univ. Press.

Gitirana, G.D.N. (2005). Weather-related Geo-hazard Assessment Model for Railway Embankment Stability. Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of Doctor of Philosophy, University of Saskatchewan, Canada.

Glaister, S. (2002). 'UK Transport Policy 1997-2001'. Oxford Review of Economic Policy, 18 (2):154-86

Gokpinar, B., Hopp, W.J., Iravani, S.M.R (2010). The Impact of Misalignment of Organisational Structure and Product Architecture on Quality in Complex Product Development. Management Science, 56(3): 468-84

Gordon, C., Mulley, C., Stevens, N., Daniels, N. (2013a). Public–private contracting and incentives for public transport: Can anything be learned from the Sydney Metro experience? Transport Policy 27: 73-84

Gordon, C., Mulley, C., Stevens, N., Daniels, N. (2013b). How optimal was the Sydney Metro contract? Comparison with international best practice. Research in Transportation Economics, 39: 239-46

Grimsey D., Lewis, K.K. (2004). Public private partnerships, Cheltenham: Edward Elgar

Grunske, L., Neumann, R. (2002). Quality improvement by integrating non-functional properties in software architecture specification. EASY'02 Second Workshop on evaluating and architecting system dependability. San Jose CA

Grunske, L., Kaiser, B., Papadopoulos, Y.I. (2005). Model-driven safety evaluation with state-event-based component failure annotations. 8th International Symposium on Component-based Software Engineering, Lecture Notes in Computer Science, 3489: 33-48.

Hammond (1996). 'The History of Cost-Benefit Analysis' Conference Paper, ASA. http://www.chicagoasa.org/downloads/CostBenefitConference2006/benefit%20cost%20history.pdf. Extracted 14-12-2009.

Hansen, M. T. (2002). Knowledge networks: Explaining effective knowledge sharing in multi-unit companies. Organic Science, 13(3): 232-48.

Harsanyi, J. (1955). Cardinal Welfare, Individualistic Ethics and Interpersonal Comparison of Utility, Journal of Political Economy, 63: 309-322

Hase, K.R. (2011). "Open Proof" for Railway Safety Software - A Potential Way-Out of Vendor Lock-in Advancing to Standardization, Transparency, and Software Security. Springer Berlin Heidelberg, 5-38.

HC (2014). Safety at level crossings: Eleventh Report of Session 2013–14. House of Commons Transport Committee, HC 680.

Hendriks, M., Voeten, B., Kroep, L. (1999). Human resource allocation in a multi-project R&D environment: resource capacity allocation and project portfolio planning in practice. International Journal of Project Management, 17: 181-8

Henley, E.J., Kumamoto, H. (1981). Reliability Engineering and Risk Assessment, Englewood Cliffs, NJ: Prentice Hall

Henry, J.J., Farges, J.L., Tuffal, J., (1983). 'The PRODYN real time traffic algorithm', Proceedings of the 4th IFAC-IFIP-IFORS Conference on Control in Transportation Systems, 307-11

Hey, J. D. (1995). Experimental investigations of errors in decision making under risk. European Economic Review, 39: 633-640

Hickling, N. (2007). An Independent Review of a Rail-Specific Human Reliability Assessment Technique for Driving Tasks (No. T270). Rail Safety and Standards Board, London.

Hill, R.J. (1997). Electric railway traction. Part 7 Electromagnetic interference in traction systems. Power Engineering, 11 (6): 259-66

Hobbs, B., Andersen, B. (2001). Different alliance relationships for project design and execution. International Journal of Project Management 19: 465-9.

Hockey, B., Carrigan, N. (2003). Human Factors in Railway Systems: Implications for Safety. Rail Research UK. The universities' centre for railway systems research. Prepared for the Railway Safety & Standards Board by, Human Factors Laboratory, School of Psychology, University of Leeds, RRUK/B2&B3/1. http://portal.railresearch.org.uk/RRUK/Shared%20Documents/rssbb2.pdf. Accessed 09-07-12.

Holzmann, V., Spiegler, I. (2011). Developing risk breakdown structure for information technology organizations. International Journal of Project Management 29: 537-46

House of Commons Select Committee on Transport, Local Government and Regions (2002) London Underground, HC 680, Session 2001-02, London: The Stationery Office

Horowitz, E., Sahni, S. (1974). Computing partitions with applications to the Knapsack Problem, Journal of the ACM, 21: 277-292

HM Treasury (2003). The Green Book – Appraisal and Evaluation in Central Government Treasury Guidance

HMRI (2006). The Railway Safety Principles and Guidance ('Blue Book') 'The Railways, the Market and the Government'. The Institute of Economic Affairs 5:21-44

HSE (1974). Health and Safety at Work etc. Act 1974. Health, Safety and Welfare in Connection with Work and Control of Dangerous Substances and certain Emissions into the Atmospheres, 37 (1).

HSE (1996). Study of Upward Flame Spread on Inclined Surfaces. HSE Contract Research Report No. 122/1996.

HSE (1997). Successful Health and Safety Management. HSG 65.

HSE (1988). The Tolerability of Risk from Nuclear Power Stations

HSE (1999). Management of Health and Safety at Work Regulations (MHSWR) 1999, No. 3242.

HSE (2000a). The Southall Rail Accident Inquiry Report.

HSE (2000b).*The train collision at Ladbroke Grove 5 October 1999* A report of the HSE investigation

HSE (2000c). The Ladbroke Grove Rail Inquiry. Part 1 Report

HSE (2000d). The management of safety in Railtrack - A review by the Health and Safety Executive

HSE (2000e). Proposed Amendments to the Railways (Safety Case) Regulations 2000. Regulatory Impact Assessment (Post-Consultation). http://www.hse.gov.uk/consult/condocs/railresult.pdf. Accessed 30-04-2011.

HSE (2001a). The Southall and Ladbroke Grove Joint Inquiry into Train Protection Systems

HSE (2001b). The Ladbroke Grove Rail Inquiry. Part 2 Report

HSE (2001c). Reducing Risks, Protecting People, HSE's decision making process

HSE (2002). Railway Safety – Assessment of Railtrack's management of multi-SPAD Signals

HSE (2005). The Rail Public Inquiries - HSC report on overall progress as of March 2005 on the remaining recommendations from the Rail Public Inquiries: The Southall Rail Accident Inquiry Report; The Joint Inquiry into Train Protection Systems; The Ladbroke Grove Rail Inquiry Part 1 Report; The Ladbroke Grove Rail Inquiry Part 2 Report http://www.railwaysarchive.co.uk/documents/HSE_Public2005.pdf. Accessed 30-04-2011

HSL (2005). An Asset Management Model for UK Railway Safety. HSL/2005/34

IEA (2006). The Railways, the Market and the Government. The Institute of Economic Affairs. Blackwell Publishing, Oxford.

IEC 61508 (2010). Functional safety of electrical/electronic/programmable electronic safety related systems, 5 (C): 24 – 26.

Johnson, C.W. (2002). Reasons for the failure of incident reporting in the healthcare and rail industries, Proceedings of the 10th Safety-Critical Systems Symposium, Berlin, Germany, 31-60.

Jones, D. (2002). Providing value for money through public private partnerships: the lessons learnt so far from economic and social infrastructure projects. In: Policy development in Australia for pubic private partnerships – what more is there to do? The Avillion Hotel, Sydney Australia; 2002: 99–107.

Jones-Lee, M. W., Loomes, G. (1995), Discounting and Safety, Oxford Economic Papers, New Series, 47(3): 5001-512.

Jones-Lee, Michael (1989). The Economics of Safety and Physical Risk. Oxford: Basil Blackwell.

Jones-Lee, Michael W. (1976). The Value of Life: An Economic Analysis. University of Chicago.

Jupe, R. (2009). New Labour, Public – Private Partnerships and rail transport policy. Economic Affairs, 29 (01): 20-25.

Kahneman, D., Tversky, A. (1979). Prospect Theory: An Analysis of Decisions under Risk, Econometrica, 47: 263-91.

Kaiser, B., Gramlich, C., Forster, M. (2007). State/event fault trees – a safety analysis model for software-controlled systems. Reliability Engineering and System Safety, 92: 1521–37.

Ke, Y., Wang, S.Q., Chan, A., Lam, P.T I. (2010). Preferred risk allocation in China's public–private partnership (PPP) projects. International Journal of Project Management, 28: 482–92.

Kelman, S. (1981). Cost-Benefit Analysis: An Ethical Critique. American Enterprise Institute Journal on Government and Society Regulation, 33-40.

Khisty, C.J., Mohammadi, J., (2001). Fundamentals of System Engineering, with Economics, Probability and Statistics. Prentice Hall, Inc., Upper Saddle River, N.J.

Kirwan, B. (1992). Human error identification in human reliability assessment Part 1: overview of approaches. Applied Ergonomics, 23(5), 299-318

Kirwan, B. (1994). A guide to practical human reliability assessment, London: Taylor and Francis.

Kleindorfer, P.R., Saad, G.H. (2005). Managing disruption risks in supply chains. Production and Operations Management 14: 53-68.

Kletz, T.A. (2005). Looking Beyond ALARP - Overcoming its Limitations. Trans IChemE, Part B, Process Safety and Environmental Protection 83(B2): 81-4.

Koppenjana, J., Veenemanb, W., Van der Voortb, H., ten Heuvelhofb, E., Leijten, M. (2011). Competing management approaches in large engineering projects: The Dutch RandstadRail project. International Journal of Project Management 29:740-50.

Kreitz, C., Hayden, M., Hickey, J. (1998). A Proof Environment for the Development of Group Communication Systems. 15th International Conference on Automated Deduction (CADE-15), 1421:317–331.

Kumar, A., Sinha, P.K. (2008). Human Error Control in Railways. Jordan Journal of Mechanical and Industrial Engineering, 2 (4): 183-190.

Kumar, S., Schmitz, S, (2011). Managing recalls in a consumer product supply chain– root cause analysis and measures to mitigate risk. International Journal of Production Research 49: 235-53.

Layard, R., Glaister, S. (1994). Cost-Benefit Analysis, Cambridge: Cambridge University Press

Lee, M.A., Flynn, B.B., Frohlich, M.T. (2008). All supply chains don't flow through: understanding supply chain issues in product recalls. Management and Organization Review, 4: 167-82.

Lee, H.L., Whang, S. (2005). Higher supply chain security with lower cost: lessons from total quality management. International Journal of Production Economics, 96: 289-300.

Lees, F.P. (1980). Loss Prevention in the Process Industries, Butterworth-Heinemann. 2 Vols.

Lees, F. (1996). Loss prevention in the process industries, Butterworth-Heinemann. 2nd Edn.

Lewis, R., Dwyer-Joyce, R.S. (2006). Wear at the wheel/rail interface when sanding is used to increase adhesion. Proceedings of the Institute of Mechanical Engineering F-J RAI, 220(1), 29-41.

Li, J., Pollard, S., Kendall, G., Soane, E., Davies, G. (2009). Optimising risk reduction: An expected utility approach for marginal risk reduction during regulatory decision making. Reliability Engineering and System Safety, 94 (11), 1729-1734

Lind, N.C., Nathwani, J.S., Siddall, E. (1991). Managing Risks in the Public Interest. Institute for Risk Research, University of Waterloo.

Lindhe, A., Rose´n, L., Norberg, T., Bergstedt, O., Pettersson, T.J.R. (2011). Cost-effectiveness analysis of risk-reduction measures to reach water safety targets. Water Research 45: 241-253.

Liu, X., Kreitz, C., van Renesse, R., Hickey, J., Hayden, M., Birman, K., Constable, R. (1999). Building reliable, high-performance communication systems from components. 17th ACM Symposium on Operating Systems Principles. Operating Systems Review, 34 (5): 80–92.

Loomes, G., Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. Economic Journal, 92: 805-824

Love, P.E.D., Lopez, R., Goh, Y.M., Tam, C.M. (2011). What goes up shouldn't come down: Learning from construction and engineering failures. The 12th East Asia-Pacific Conference on Structural Engineering and Construction. Procedia Engineering, 14: 844-50.

Lindman, H.R. (1974). Analysis of variance in complex experimental designs. San Francisco: W. H. Freeman & Co.

Liu, T., Wilkinson, S. (2013a). Large-scale public venue development and the application of Public–Private Partnerships (PPPs). International Journal of Project Management, 32(1), 88-100.

Liu, T., Wilkinson, S. (2013b) Can the pilot Public-Private Partnerships project be applied in future urban rail development? A Case Study of Beijing Metro Line 4 Project, Built Environment Project and Asset Management, 3 (2): 250-263.

Lockamy III, A., McCormack, K. (2004). The development of a supply chain management process maturity model using the concepts of business process orientation", Supply Chain Management: An international Journal, 9 (4):272-78.

Loomes, G., Sugden, R. (1982). Regret theory: An alternative theory of rational choice under uncertainty. Economic Journal, 92: 805-824.

Love, P.E.D., Lopez, R., Goh, Y.M., Tam, C.M. (2011). What goes up shouldn't come down: Learning from construction and engineering failures. The 12th East Asia-Pacific Conference on Structural Engineering and Construction. Procedia Engineering 14: 844-850.

LUL (2012). London Underground Safety Certificate and Safety Authorisation version 2.0. http://beta.tfl.gov.uk/cdn/static/cms/documents/safety-certification-complete.pdf. Accessed 11-11-2013

Maciariello, J.A. (1975). Dynamic Benefit-Cost Analysis – Evaluation of Public Policy in a Dynamic Urban Model. Massachusetts: D.C. Heath and Company.

Maisel, W.H., 2005. Safety issues involving medical devices: implications of recent implantable carioverter-defibrillator malfunctions. Journal of the American Medical Association 294, 955-58

Manpreet, H., Bapuji H., Roth A. V. (2011). Safety hazard and time to recall: The role of recall strategy, product defect type and supply chain player in the U.S. toy industry. Journal of Operations Management 29: 766-77

Markowitz, H.M. (1952). Portfolio Selection. Journal of Finance 7 (1): 77-91

Marschak, J. (1950). 'Rational Behavior, Uncertain Prospects, and Measurable Utility', Econometrica, 18: 111-41.

Marshal, C. (2001). Measuring and Managing Operational Risk in Financial Institutions, Hoboken NJ: John Wiley & Sons.

Maruchek, A., Greis, N., Mena C., Cai L. (2011). Product safety and security in the global supply chain: Issues, challenges and research opportunities. Journal of Operations Management 29: 707-20

Matthews J., Rowlinson S. (1999) Partnering: Incorporating Safety Management. Engineering, Construction and Architectural Management 6 (4): 347-57.

Mauriello, A.J. and Clarke, J.M., (1983). Measurement and analysis of radiated electromagnetic emissions from rail-transit vehicles. IEE Transactions on Electromagnetic Compatibility 25 (4): 405-11

McFarlan, F.W. (1992). 'Multinational CIO challenges for the 199Os', in Palvia, S., Palvia, P. and Zigli, R.M. eds, The Global Issues of Information Technology Management, Harrisburg PA: Idea Group Publishing

Medda, F. (2007). A game theory approach for the allocation of risks in transport public private partnerships. International Journal of Project Management 25 (3): 213-18

Menard, S. (1995). Applied Logistic Regression Analysis, Thousand Oaks, CA: Sage Publications

Millera, R., Lessard, D. (2001). Understanding and managing risks in large engineering projects. International Journal of Project Management 19: 437-43

Minhyung, K. (2010). Risks of Global Production Systems: Lessons from Toyota's Mass Recalls. SERI Quarterly, http://www.faqs.org/periodicals/201007/2089147441.html. Accessed 09-08- 2013

Mishan, E.J. (1976). Cost Benefit Analysis New York: Praeger, 3rd Edn.

Mishan, E.J., Quah, E. (2007). Cost-Benefit Analysis, 5th Edition. London: Taylor & Francis

Moore W.B., Muller T. (1989). Impacts of development and infrastructure financing. Journal of Urban Planning and Development 115 (2):95-108.

Narasimhan, R., Talluri, S. (2009). Perspectives on risk management in supply chains. Journal of Operations Management 27: 114-18

Nash, C.A. (2002): 'Regulatory Reform in Rail Transport - the UK experience', Swedish Economic Policy Review, 9 (2): 257-86.

Nave, M., Veltri, A. (2004). Effect of loss control services on reported injury accidents. Journal of Safety Research 35: 39-46.

Neil, M., Fenton, N. (2005). Tailor M. Using Bayesian networks to model expected and unexpected operational losses. Risk Analysis, 25: 963–72.

Neter, J., Kutner, M.H. Nachtsheim, C.J., Wasserman, W. (1996). Applied Linear Statistical Models, New York: McGraw-Hill.

Newman, T. B. (2003). The power of stories over statistics. The British Medical Journal, 327: 1424-7.

Ng, A., Loosemore M. (2007). Risk allocation in the private provision of public infrastructure. International Journal of Project Management 25:66–76.

Nobeoka, K., Cusumano, M. (1995). Multi-project strategy, design transfer, and project performance: a survey of automobile development projects in the US and Japan. IEEE Transactions, Engineering Management (42): 397-409.

Nonaka, I., Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. New York: Oxford University Press.

Nordland, O. (2001). When is risk acceptable? The 19th International System Safety Conference – A System Safety Odyssey, Huntsville, Alabama.

Olivier A., Nicolas T. (2004). Social Willingness to Pay, Mortality Risks and Contingent Valuation. The Journal of Risk and Uncertainty, 29 (1): 7-19.

Olson, D. L. (1988). Opportunities and Limitations of AHP in Multi-objective Programming. Math Computing Modelling, 11: 206-209

ORR (2002). Train Derailment at Porters Bar – Friday 10 May 2012, HSE Interim Report – 14th May 2002. http://webarchive.nationalarchives.gov.uk/20131001175041/http://www.rail-reg.gov.uk/upload/pdf/incident-pottersbar-interim.pdf. Accessed 22-01-12

ORR (2003). Train Derailment at Porters Bar 10 May 2002 - A Progress Report by the HSE Investigation Board, 55 – 58. http://webarchive.nationalarchives.gov.uk/20131001175041/http://www.rail-reg.gov.uk/upload/pdf/incident-pottersbar-may03progrep.pdf. Accessed 22-01-12.

ORR (2010). Monitoring and Evaluation of Railways and Other Guided Transport Systems (Safety) Regulations (ROGS). http://orr.gov.uk/__data/assets/pdf_file/0017/2591/rogs-monitor-bomel-reprt-nov08.pdf. Accessed 03-05-12.

ORR (2013). Railways and Other Guided Transport Systems (Safety) Regulations (ROGS). http://www.rail-reg.gov.uk/server/show/nav.1511. Accessed 29-10-13

Ozkir, V., Demirel, T. (2012). A fuzzy assessment framework to select among transportation projects in Turkey. Expert Systems with Applications, 39: 74–80.

Papadopoulos, Y., Walker, M., Parker, D., Rüde, E., Hamann, R., Uhlig, A., Grätz, U., Lien, R. (2011). Engineering failure analysis and design optimisation with HiP-HOPS. Engineering Failure Analysis 18: 590-608.

Patanakul, P., Milosevic, D. (2009). The effectiveness in managing a group of multiple projects: Factors of influence and measurement criteria. International Journal of Project Management 27: 216-33

Peleska, J., Feuser, J., Haxthausen, A.E. (2012). The Model-Driven openETCS Paradigm for Secure, Safe and Certifiable Train Control Systems. In Flammini, Francesco (ed.). "Railway Safety, Reliability, and Security: Technologies and Systems Engineering." IGI Global, 22-52.

Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies. Princeton NJ: Princeton University Press.

Persaud, B., Kazakov, A. (1994). A procedure for allocating a safety improvement budget among treatment types. Accident Analysis and Prevention, 26(1):121-126

Pham, H. T.V., Fredlund, D.G. (2003). The Application of Dynamic Programming to slope stability analysis. Canadian Geotechnical Journal, 40: 830-47

Pirlot, M. (1996). General local search methods. European Journal of Operational Research, 92: 493-511.

Powell, W.B. (2007). Approximate Dynamic Programming: Solving the Curses of Dimensionality. Hoboken NJ: John Wiley & Sons, Inc.

Pyke, D., Tang, C.S. (2010). How to mitigate product safety risks proactively? Process, challenges and opportunities. International Journal of Logistics Research and Applications: A Leading Journal of Supply Chain Management 13: 243-56.

Royal Academy of Engineering [RAE] (2000). Automatic Train Protection for the Railway Network in Britain – A study.

Rangel, T., Vassallo, J-M, Arenas, B. (2012). Effectiveness of safety-based incentives in Public Private Partnerships: Evidence from the case of Spain. Transportation Research Part A 46: 1166-76

Railways Act 2005. The Stationery Office Limited

Rail Safety and Standard Board [RSSB] (2003): Risk Profile Bulletin, Profile of Safety Risk on the UK Mainline Railway. Issue 3, Railway Safety

Ramanathan, R., Ganesh, L.S. (1995). Using AHP for resource allocation problems. European. Journal of Operational Research, 80: 417.

Rashid, M., Hayes, D.F. (2011). Needs-based sewerage prioritization: Alternative to conventional cost-benefit analysis. Journal of Environmental Management, 92: 2427-40.

Remenyi, D., Heafield, A. (1996). Business process re-engineering: some aspects of how to evaluate and manage the risk exposure. International Journal of Project Management 14 (6): 349-57

Robin, B. (1974). The Welfare Foundations of Cost-Benefit Analysis, Economic Journal 84(336): 926-39

Rothenberg, J. (1961). The Measurement of Social Welfare. Prentice-Hall, Englewood Cliffs, NJ

RSSB (2005a). The Railway Strategic Safety Plan 2005.http://www.rssb.co.uk. Accessed 02-06-2011

RSSB (2005b). The Rail Safety and Standard Board: Annual Safety Performance Report 2005. http://www.rssb.co.uk. Accessed 02-06-2011

RSSB (2006). Assessment of the Value of Preventing Fatality VPF Phase I. T430 – Definition of VPF & the Impact of Societal Concerns. http://www.rssb.co.uk/. Accessed 21-03-13

RSSB (2007). The Railway Strategic Safety Plan 2007-2009. http://www.rssb.co.uk/sitecollectiondocuments/pdf/reports/strategic_safety_plan_07-09.pdf. Accessed 28-05-2011.

RSSB (2008). The Rail Safety and Standard Board: The Railway Strategic Safety Plan 2008 – 2010. http://www.rssb.co.uk/SiteCollectionDocuments/pdf/reports/strategic%20safety%20plan.pdf. Accessed 02-06-2011.

RSSB (2010). The Railway Safety and Standards Board Annual Safety Performance Report 2009/10. A reference guide to safety trends on GB railways. http://www.rssb.co.uk/sitecollectiondocuments/pdf/reports/ASPR_2009_10_Full_Report.pdf. Accessed 02-06-2011

Saaty, T. (1988). The Analytic Hierarchy Process, McGraw-Hill, New York.

Saltelli, A., Bolado B. (1998). 'An Alternative Way to Compute Fourier Amplitude Sensitivity Test (FAST),' Computational Statistics and Data Analysis, 26(4): 445-60

Sato, Y. (2012). "Optimal budget planning for investment in safety measures of a chemical company". International Journal of Production Economics, 140: 579-585.

Sarathy, R., (2006). Security and the global supply chain. Transportation Journal, 45 (4), 28–51

Schlindwein, S.L.; Ison, R. (2004). Human knowing and perceived complexity: implications for systems practice. Emergence: Complexity and Organization 6: 27–32

Schmeidler, D. (1989). Subjective probability and expected utility without additivity. Econometrica 57(3): 571-87

Schmid, A.A. (1989). Benefit-Cost Analysis – Political Economy Approach, Boulder CO: Westview Press Inc.

Schroeder M. (2006). Developing Cem Design Standards To Improve Light Rail Vehicle Crashworthiness. in Proceedings of JRC2006. [Joint Rail Conference], April 4-6, Atlanta GA.

Seider, R. (2006). Optimizing project portfolios. Research Technology Management, 49 (6): 43-48.

Shaofeng, L. (2011). Optimising Power management Strategies for Railway Traction Systems. Thesis submitted to the University of Birmingham for the degree of Doctor of Philosophy.

Shaoul, J. (2002) New Developments: A Financial Appraisal of the London Underground Public-Private Partnership, Public Money & Management, 22 (2): 53-60

Shehzad, F., Ali Shah, M.A. (2009). Evaluation of Shortest Paths in Road Network. Pakistan Journal of Commerce and Social Sciences 3: 67-79.

Silverman H., Morgan D. (1990). The Application of Dynamic Programming to Connected Speech Recognition. IEEE ASSP Magazine Network. 7 (3): 6 – 25.

Šimić, Z., Mikuličić, V., Vuković, I. (2007). Proceedings of the NATO Advanced Research Workshop on Computational Models of Risks to Infrastructure, Primosten, Croatia: 216-25.

Sniedovich, M.B. (1978). Dynamic Programming and Principles of Optimality. Journal of Mathematical Analysis and Applications, 65: 586-606

Spouge, J. (1999). A guide for Quantitative Risk Assessment for Offshore Installations, Aberdeen: CMPT

Stanton, N. A., Salmon, P. M., Walker, G. H., Baber, C., Jenkins, D. P. (2005). Human Factors Methods: A Practical Guide for Engineering and Design. Ashgate Aldershot.

Star, C. (1969). Social Benefits versus Technological Risks. Science, 165 (3899): 1232–1238

Taleb, N.N. (2007). The black swan, the impact of the highly improbable, Harmondsworth: Penguin Books.

Tang, C.S. (2006). Perspectives in supply chain risk management. International Journal of Production Economics, 103: 451-88.

Tingting, L., Wilkinson S. (2013). Large-scale public venue development and the application of Public–Private Partnerships (PPPs). International Journal of Project Management 32(1):88–100.

Todinov, M.T. (2001). The limitations of maximum expected utility principle as a basis for rational risk decisions. Reliability, Risk and Safety: Theory and Applications. London: Taylor & Francis

Todinov, M. T. (2006). Reliability Analysis Based on the Losses from Failures. Risk Analysis, 26 (2): 311-35.

Todinov, M. T. (2007) Risk-based reliability analysis and generic principles for risk reduction. Atlanta GA: Elsevier.

Todinov M.T., Weli E. (2013). Optimal risk reduction in the railway industry by using dynamic programming. International Conference on Reliability, Safety and Security Engineering, London, UK. World Academy of Science Engineering and Technology, 79: 220-24.

Trevor, C., Chilton, S., Hopkins, L., Jones-Lee, M., Loomes, G., Pidgeon, N., Spencer, A. (1998). On the Contingent Valuation of Safety and the Safety of Contingent Valuation: Part 2 – The CV/SG 'Chained' Approach, Journal of Risk and Uncertainty, 17: 187-213

Tsitsiklis J. N., van Roy, B. (1999). 'Optimal Stopping of Markov Processes: Hilbert Space Theory, Approximation Algorithms, and an Application to Pricing Financial Derivatives', IEEE Transactions on Automatic Control, 44 (10): 1840-51

Tung, A. B., Kaur K., Bhadauria S., (2013). Dynamic Programming Model based on Cost Minimization algorithms for Thermal Generating Units. International Journal of Enhanced Research In Science Technology & Engineering, 1 (1): 58-64.

Tversky, A., Kahneman, D. (1992). Advances in Prospect Theory: Cumulative representation of uncertainty. Journal of Risk and Uncertainty 5: 297-323.

Taleb, N.N. (2007). The black swan, the impact of the highly improbable. Harmondsworth: Penguin books.

Turner, S., Keeley, D., Glossop, M., Brownless, G. (2002). A Review of Railway Safety's Safety Risk Model HSL report: HSL/2002/06.

van Der Merwe, A.P. (2002a). Project Management and business development: integrating strategy, structure processes and projects International Journal of Project Management 20: 401-411.

Van Der Merwe, A.P. (2002b). Multi-project management - organizational structure and control. International Journal of Project Management, 15 (4): 223-33.

Van Laarhoven, P. J. M., Aarts, E. H. L., Lenstra, J.K. (1992). "Jobshop scheduling by simulated annealing". Operations Research, 40: 113-125.

Van Welie, M., Van Der Veer, G. (2003). Groupware Task Analysis. In E. Hollnagel (Ed) Handbook of Cognitive Task Design. Lawrence Erlbaum Associates, 447 - 477.

Veltri, A., Dance, D., Nave, M. (2003a). Safety, health and environmental cost model: An internal study from the semiconductor manufacturing industry (Part 1). Professional Safety, 48 (7): 30-36.

Veltri, A., Dance, D., Nave, M. (2003b). Safety, health and environmental cost model: An internal study from the semiconductor manufacturing industry (Part 2). Professional Safety, 48 (8): 23-32.

Veltri, A., Ramsay, J., (2009). Economic Analysis – Make the Business Case for SH&E Professional Safety. The Journal of the American Society of Safety Engineers, 9: 22-30.

Vidal, L. A., Marle, F., Bocquet, J.C. (2011). Using a Delphi process and the analytic hierarchy process (AHP) to evaluate the complexity of projects Expert Systems with Applications, 38 (5): 388-405.

von Neuman, J. , Morgenstern, O. (1947). The Theory of Games and Economic Theory Princeton: Princeton University Press.

von Winterfeldt, D., Edwards W. (1986). Decision Analysis and Behavioural Research Cambridge: Cambridge University Press.

Vose, D. (2000). Risk analysis - a quantitative guide Hoboken NJ: John Wiley & Sons, 2nd edn.

Wagner, S. M., Bode C. (2006). An empirical investigation into supply chain vulnerability Journal of Purchasing & Supply Management, 12: 301-12.

Weale, M. (2009). A Cost-Benefit Analysis of Cataract Surgery Based on the English Longitudinal Survey of Ageing', National Institute of Economic and Social Research, NIESR Discussion Paper 349.

Weli, E., Todinov, M.T. (2013a). A new approach to risk reduction in the railway industry. Institution of Engineering and Technology Special Interest Publication - Infrastructure Risk & Resilience: Transportation, 47 – 52.

Weli E., Todinov, M.T. (2013b). A new classification of risk-reduction options to improve the risk-reduction readiness of the railway industry. International Journal of Social, Human Science and Engineering, 7 (9): 858 – 867.

Whitty, S.J., Maylor, H. (2009). And then came complex project management. International Journal of Project Management 27: 304-10.

Willcocks, .L., Margetts, H. (1991). Informatization in UK public services from implementation through strategy, to management. EPGA Conference – Informatization in Public Administration, The Hague, Netherlands.

Williams, T., Eden, C., Ackermann, F., Tait, A. (1995). The effects of design changes and delays on project costs. Journal of the Operational Research Society, 809-18.

Winer, B.J. Brown, D.R. Michels, K.M. (1991) Statistical Principles in Experimental Design New York: McGraw-Hill Inc., 3rd edn.

Wolmar, C. (1996). The Great British Railway Disaster. How Privatisation Wrecked Britain's Railways Birmingham: Ian Allan Publishing.

Wolmar, C (2001). Broken Rails: How Privatisation Wrecked Britain's Railways London: Aurum Press.

Wolmar, C. (2005). On the Wrong Line: How Ideology and Incompetence Wrecked Britain's Railways London: Aurum Press.

Wong, V., Shaw, V., Sher, P. J. H. (1998). Effective Organization and Management of Technology Assimilation - The Case of Taiwanese Information Technology Firms. Industrial Marketing Management 27: 213-27.

Wood, R.T. (2010). Diversity Strategies to Mitigate Postulated Common Cause Failure Vulnerabilities. Seventh American Nuclear Society International - Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, American Nuclear Society.

Wu, Y., Drysdale, D. D. (1996). HSE Contract Research Report No. 122/1996. Study of Upward Flame Spread on Inclined Surfaces.

Young, V., Shorrock, S., Faulkner J., Braithewaite G. (2004). Who moved my (Swiss) cheese? The (r)evolution of human factors in transport safety investigation. Human Factors in Investigation, International Society of Air Safety Investigators Annual Conference, (ISASI), Australia.

Zaltman, G., Dunca, R., Holbeck, J. (1973). Innovations and Organizations New York: Wiley.

APPENDIX A: Comprehensive set of risk reduction measures for railway accidents (preventive and protective measures)

APPENDIX A1: Risk reduction measures for 'Collision Between Trains' accidents

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
Collision Between Trains	**Brake trigger system failure**	*Improve braking systems*	•	•			•	•						•				•	•					•					Preventive
		Replacement of brake controllers	•	•			•	•										•	•					•					Preventive
		Renewal of brake valves	•	•															•										Preventive
		Additional testing and inspection - improve test and inspection regimes (specifically brake systems) prior to						•	•			•	•													•			Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		deployment																											
		Driver training on the use of emergency braking (deadman handle)									•			•										•	•				Dual
		Introduction of alternative / automatic braking systems to improve availability of braking systems	•	•	•		•	•					•	•				•	•					•					Preventive
		Introduction of brake failure alarms or detection systems			•								•													•			Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
	Train slow or stopped	*EMC studies, monitoring interference levels*						•					•													•			Preventive
		Traction system renewal/re-furbishment					•	•							•						•								Preventive
		Improvement of processes/procedures (including driver training)						•			•			•	•									•					Preventive
		Further/enhanced/additional operational railway testing prior to operations on live track						•	•			•	•	•	•											•			Preventive
	Train runs away	*Re-assessment of stabling procedures - potentially leading to*					•	•			•			•										•	•				Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		change in stabling procedures and subsequently training of depot staff and train drivers																										
		Improve testing and maintenance regime for trainstop, parking brakes for all stabling points						•	•			•														•			Preventive
		Enhanced testing and maintenance regime for spring applied parking brakes to eliminate/reduce WSF of the						•	•			•														•			Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		spring applied parking brakes																											
		Relocation of stabling points - from downslope locations					•	•								•													Preventive
		Improved communication between line controller and drivers/operators					•	•						•								•			•				Dual
	SCAT failure	*Replace with improved speed sensing equipment*	•	•				•						•			•		•										Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		SCAT system inspected/tested prior to train leaving the depot - improved SCAT inspection and testing regime						•	•			•													•			Preventive
	Wrong direction	*Modification of train movement procedures and driver training - improved additional training and driver behavioural studies/assessments*						•	•			•											•	•				Preventive
		Extensive sighting studies to identify potential					•							•													•		Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		sighting problems																											
		Modification of signalling in line with sighting constraints					•	•						•				•			•								Preventive
		Change to single stopping positions						•						•									•		•				Preventive
		Introduction and use of in-cab CCTV eliminating/reducing other person induced constraints on stopping positions		•										•									•						Preventive
		Introducing train stops in areas where they currently don't	•					•																	•				Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		exist																											
		Introduction of enhanced technology such as radar/alarm systems	•					•																•		•			Dual
		Additional supervision to check the aspect prior to the reverse movement		•				•						•									•						Preventive
	Side Swipe	*Track re-alignment to guage (focus on track stressing & effects of weather on embankment and structures*						•	•												•								Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Speed restrictions - side swipe						•		•				•									•		•				Preventive
	Service brake failure	*Onboard sanding*				•				•						•							•		•				Protective
		Driver training - braking techniques									•			•										•					Preventive
		Notices on slippery routes						•		•																•			Preventive
		Alarm/Audible warning of service brake failure prior to brake demand						•						•												•			Preventive
	Signal WSF	*Berth track diversity*	•	•				•						•					•										Preventive
	Compromised overlap	*Speed restriction - Compromised overlaps*						•		•				•									•		•				Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Overlap studies and potential extension of overlaps	•	•				•														•						Preventive
		Enhance braking performance (See 'Improved braking system' above)	•	•			•	•						•				•	•					•					Preventive
		Studies on effect of power in trains (especially for the introduction of new trains) and potentially driver training on specific areas of compromised overlaps (controlling trains - traction power						•			•																•		Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		management)																											
		Driver training - SPAD												•										•					Dual
		Train speed restrictions - likely SPAD locations (Signal Sighting)					•	•		•													•		•				Preventive
	Poor Wheel/Rail Friction	*Vegetation management programme - leaf fall (autumn season specific challenge)*						•															•		•				Protective
		Fitting of wheel slip protection or Adhesion improvers						•															•		•				Protective

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		On-board sanding (see also 'Service Brake Failure')				•		•		•						•							•		•				Dual
		Increased overlap in the design of the signalling system - extension of overlaps						•						•	•						•								Preventive
		Introduction of weather forecasting/predictive systems such as ACAT						•						•													•		Preventive
		Water jetting and sandite						•					•	•		•										•				Preventive
		Wheel rim scrubbers						•	•							•										•				Dual

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Anti-icing trains - spraying heated anti-freeze onto the affected areas						•		•						•									•				Dual
		Procedures (also covering changes to operational concept) and subsequent driver and relevant railway driver training						•						•										•					Preventive
	Driver passed signal at danger (SPAD)	*Train arrestor assessment and deployment/installation*											•	•		•								•					Dual
		Extend operational testing prior to						•		•		•														•			Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		service for tripcocks, arrestors and SPAD control systems																											
		Emergency timetable - contingency plan for dealing with severe disruption (production of emergency timetables and dissemination of timetable information to all personnel especially operational personnel following an accident)									•						•				•	•	•	•	•				Protective

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Driver training - additional procedures to support drivers (SPAD)						•						•										•					Preventive
		SPAD incident plan (immediate detection and action on signals passed at danger to reduce the consequence of failure)						•						•								•	•	•	•				Protective
		Crash worthiness and vehicle interior						•								•	•	•											Protective
		ATC system introduction	•	•	•		•	•						•				•	•	•				•					Preventive
		New/enhanced interlocking system - route locking system	•	•	•		•	•						•				•	•				•		•				Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Introduction of automatic signalling systems - minimisation of human error												•	•														Preventive
		TPWS Train Protection and Warning System	•	•	•		•	•						•				•	•						•				Preventive
		Modify signalling to align with sighting constraints					•	•						•				•			•								Preventive
		Speed restrictions (Adhesion)						•				•											•	•	•				Protective
		Additional testing and inspection of wheels and rail (NDT)						•		•																•			Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Tripcock positions to be re-examined and potential relocation/re-installation		•				•								•												Preventive
		Exhaustive network survey to identify potential sighting issues						•																		•			Dual
		Extend overlaps						•	•			•			•							•							Preventive
	Emergency brakes fail to apply	*Additional testing of brakes to determine if brakes are isolated*						•	•			•														•			Preventive
		Precautions, procedural modifications and												•										•	•				Protective

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		subsequently, driver training for running with isolated emergency brakes																											
		Introduction of enhanced braking system - eliminate scenarios where emergency brake signals fail to transmit to brakes (Same as 'improved braking' above)		•	•		•	•		•	•	•						•	•			•	•	•					Preventive
		Assess the emergency brake performance of trains										•															•		Dual

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Training for maintenance and test teams						•						•									•						Preventive
		Additional operational testing and inclusion in regime for rigorous asset acceptance/approval						•	•			•														•			Preventive
		introduction of advanced radio/comms network across line section										•													•				Dual
	Delayed communications due to train radio system	*Rewiring/refurbishment of existing comms/radio systems*					•							•							•								Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Better communication between train drivers and line controllers - comms procedure/driver and line controller training	•	•			•	•																					Preventive
		Update communication procedure and related procedures for drivers and line controllers						•				•															•		Preventive
		Modify the train traction system e.g. filters, ICMU (Interference Current Monitoring Unit)	•	•	•		•	•						•				•											Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
	Traction power or track circuit of adjacent line not indicating occupied or showing shorted by derailed train	*Extended overlap*		•				•														•							Preventive
	Wrong direction train movement (due to 1. Signal Operator error and 2. Driver error)	*Emergency accident/incident plans*												•	•								•	•	•				Protective
	Collision with another train subsequent to a collision.	*Incident team on site - trained incident stations staff availability*												•	•								•	•	•				Protective

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
	[Both incident train drivers incapacitated (fast collision)]	*Training for drivers and incident centre personnel*												•										•	•				Protective
		Training for local emergency medical team on train accidents /incidents												•										•	•				Protective
		Additional procedures and subsequently, Driver and Signal Operator training - observation that wrong route is set prior to proceeding past signal						•			•			•										•	•				Preventive

Major Accident	Contributors	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles													Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operation	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways to escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems for degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Audible warning systems - trains																						•				•	Protective
		Points machine failure - new/enhanced point machines with 'route holding diversity'	•	•			•							•					•										Preventive

Major Accident	Contributors	Risk Reduction Options	% reduction achieved	Accident cost (£)	Cost (£)	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
Collision Between Trains	**Brake trigger system failure**	*Improve braking systems*	0.9	6.18E+07	7.00E+06	5.48E+07	4.94E+07	7.05E+00	Preventive	Design	D-01A
		Replacement of brake controllers	0.75	6.18E+07	6.00E+06	5.58E+07	4.19E+07	6.98E+00	Preventive	Design	D-02A
		Renewal of brake valves	0.6	6.18E+07	3.00E+06	5.88E+07	3.53E+07	1.18E+01	Preventive	Design	D-03A
		Additional testing and inspection - improve test and inspection regimes (specifically brake systems) prior to deployment	0.08	6.18E+07	5.00E+06	5.68E+07	4.55E+06	9.09E-01	Preventive	Technical	T-01
		Driver training on the use of emergency braking (dead-man handle)	0.2	6.18E+07	1.00E+06	6.08E+07	1.22E+07	1.22E+01	Dual	Procedural	P-01A
		Introduction of alternative / automatic braking systems to improve availability of braking systems	0.9	6.18E+07	4.50E+06	5.73E+07	5.16E+07	1.15E+01	Preventive	Design	D-04A
		Introduction of brake failure alarms or detection systems	0.3	6.18E+07	4.00E+06	5.78E+07	1.74E+07	4.34E+00	Preventive	Design	D-05A
	Train slow or stopped	*EMC studies, monitoring interference levels*	0.08	1.24E+07	1.00E+06	1.14E+07	9.09E+05	9.09E-01	Preventive	Procedural	P-02
		Traction system renewal/refurbishment	0.8	1.24E+07	5.00E+06	7.37E+06	5.89E+06	1.18E+00	Preventive	Technical	T-02
		Improvement of processes/procedures (including driver training)	0.15	1.24E+07	1.00E+06	1.14E+07	1.71E+06	1.71E+00	Preventive	Procedural	P-03
		Further/enhanced/additional operational railway testing prior to operations on live track	0.1	1.24E+07	5.00E+06	7.37E+06	7.37E+05	1.47E-01	Preventive	Technical	T-03
	Train runs away	*Re-assessment of stabling procedures - potentially leading to change in stabling procedures and subsequently training of depot staff and train drivers*	0.15	1.24E+07	1.50E+06	1.09E+07	1.63E+06	1.09E+00	Dual	Procedural	P-04
		Improve testing and maintenance regime for train-stop, parking brakes for all stabling points	0.2	1.24E+07	5.00E+06	7.37E+06	1.47E+06	2.95E-01	Preventive	Technical	T-04
		Enhanced testing and maintenance regime for spring applied parking brakes to eliminate/reduce WSF of the spring applied parking brakes	0.15	1.24E+07	5.00E+06	7.37E+06	1.11E+06	2.21E-01	Preventive	Technical	T-05
		Relocation of stabling points - from downslope locations	0.1	1.24E+07	5.50E+06	6.87E+06	6.87E+05	1.25E-01	Preventive	Technical	T-06

Major Accident	Contributors	Risk Reduction Options	% reduction achieved	Accident cost (£)	Cost (£)	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
		Improved communication between line controller and drivers/operators	0.3	1.24E+07	1.00E+06	1.14E+07	3.41E+06	3.41E+00	Dual	Operational	O-01A
	SCAT failure	*Replace with improved speed sensing equipment*	0.8	3.71E+07	1.20E+07	2.51E+07	2.01E+07	1.67E+00	Preventive	Design	D-08
		SCAT system inspected/tested prior to train leaving the depot - improved SCAT inspection and testing regime	0.1	3.71E+07	1.00E+07	2.71E+07	2.71E+06	2.71E-01	Preventive	Technical	T-07
	Wrong direction	*Modification of train movement procedures and driver training - improved additional training and driver behavioural studies/assessments*	0.15	6.18E+07	3.00E+06	5.88E+07	8.83E+06	2.94E+00	Preventive	Procedural	P-05
		Extensive sighting studies to identify potential sighting problems	0.1	6.18E+07	1.00E+06	6.08E+07	6.08E+06	6.08E+00	Preventive	Technical	T-08A
		Modification of signalling in line with sighting constraints	0.6	6.18E+07	4.00E+07	2.18E+07	1.31E+07	3.28E-01	Preventive	Design	D-09A
		Change to single stopping positions	0.2	6.18E+07	5.00E+06	5.68E+07	1.14E+07	2.27E+00	Preventive	Technical	T-09
		Introduction and use of in-cab CCTV eliminating/reducing other person induced constraints on stopping positions	0.4	6.18E+07	3.00E+07	3.18E+07	1.27E+07	4.25E-01	Preventive	Design	D-10
		Introducing train stops in areas where they currently don't exist	0.3	6.18E+07	7.00E+06	5.48E+07	1.65E+07	2.35E+00	Preventive	Design	D-11
		Introduction of enhanced technology such as radar/alarm systems	0.2	6.18E+07	7.00E+06	5.48E+07	1.10E+07	1.57E+00	Dual	Design	D-12
		Additional supervision to check the aspect prior to the reverse movement	0.3	6.18E+07	1.00E+06	6.08E+07	1.83E+07	1.83E+01	Preventive	Operational	O-02
	Side Swipe	*Track re-alignment to gauge (focus on track stressing & effects of weather on embankment and structures*	0.8	6.18E+07	1.00E+07	5.18E+07	4.15E+07	4.15E+00	Preventive	Design	D-14
		Speed restrictions - side swipe	0.3	6.18E+07	5.00E+06	5.68E+07	1.71E+07	3.41E+00	Preventive	Operational	O-03A
	Service brake failure	*On-board sanding*	0.1	6.18E+07	2.00E+06	5.98E+07	5.98E+06	2.99E+00	Protective	Technical	T-10A
		Driver training - braking techniques	0.2	6.18E+07	1.00E+06	6.08E+07	1.22E+07	1.22E+01	Preventive	Procedural	P-01B
		Notices on slippery routes	0.05	6.18E+07	1.00E+06	6.08E+07	3.04E+06	3.04E+00	Preventive	Operational	O-04
		Alarm/Audible warning of service brake failure prior to brake demand	0.2	6.18E+07	3.00E+06	5.88E+07	1.18E+07	3.92E+00	Preventive	Design	D-15

Major Accident	Contributors	Risk Reduction Options	% reduction achieved	Accident cost (£)	Cost (£)	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
	Signal WSF	*Berth track diversity*	0.3	1.24E+08	2.00E+07	1.04E+08	3.11E+07	1.56E+00	Preventive	Design	D-16A
	Compromised overlap	*Speed restriction - Compromised overlaps*	0.3	6.18E+07	5.00E+06	5.68E+07	1.71E+07	3.41E+00	Preventive	Operational	O-03B
		Overlap studies and potential extension of overlaps	0.1	6.18E+07	3.00E+06	5.88E+07	5.88E+06	1.96E+00	Preventive	Technical	T-11A
		Enhance braking performance (See 'Improved braking system' above)	0.4	6.18E+07	7.00E+06	5.48E+07	2.19E+07	3.13E+00	Preventive	Design	D-01B
		Studies on effect of power in trains (especially for the introduction of new trains) and potentially driver training on specific areas of compromised overlaps (controlling trains - traction power management)	0.05	6.18E+07	1.00E+06	6.08E+07	3.04E+06	3.04E+00	Preventive	Technical	T-12
		Driver training - SPAD	0.3	6.18E+07	3.00E+06	5.88E+07	1.77E+07	5.88E+00	Dual	Procedural	P-01C
		Train speed restrictions - likely SPAD locations (Signal Sighting)	0.4	6.18E+07	5.00E+06	5.68E+07	2.27E+07	4.55E+00	Preventive	Operational	O-03C
	Poor Wheel/Rail Friction	*Vegetation management programme - leaf fall (autumn season specific challenge)*	0.3	1.24E+08	5.00E+06	1.19E+08	3.56E+07	7.12E+00	Protective	Operational	O-07
		Fitting of wheel slip protection or Adhesion improvers	0.1	1.24E+08	2.20E+06	1.21E+08	1.21E+07	5.52E+00	Protective	Design	D-17
		On-board sanding (see also 'Service Brake Failure')	0.1	1.24E+08	2.00E+06	1.22E+08	1.22E+07	6.08E+00	Dual	Technical	T-10B
		Increased overlap in the design of the signalling system - extension of overlaps	0.1	1.24E+08	3.00E+06	1.21E+08	1.21E+07	4.02E+00	Preventive	Technical	T-11B
		Introduction of weather forecasting/predictive systems such as ACAT	0.05	1.24E+08	5.00E+05	1.23E+08	6.16E+06	1.23E+01	Preventive	Technical	T-42
		Water jetting and sandite	0.1	1.24E+08	2.00E+06	1.22E+08	1.22E+07	6.08E+00	Preventive	Technical	T-12A
		Wheel rim scrubbers	0.01	1.24E+08	2.00E+05	1.23E+08	1.23E+06	6.17E+00	Dual	Design	D-18
		Anti-icing trains - spraying heated anti-freeze onto the affected areas	0.05	1.24E+08	4.00E+06	1.20E+08	5.98E+06	1.50E+00	Dual	Technical	T-13
		Procedures (also covering changes to operational concept) and subsequent driver and relevant railway driver	0.4	1.24E+08	5.00E+06	1.19E+08	4.75E+07	9.49E+00	Preventive	Procedural	P-01D

Major Accident	Contributors	Risk Reduction Options	% reduction achieved	Accident cost (£)	Cost (£)	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
		training									
	Driver passed signal at danger (SPAD)	*Train arrestor assessment and deployment/installation*	0.6	3.09E+08	2.00E+07	2.89E+08	1.74E+08	8.68E+00	Dual	Technical	T-14
		Extend operational testing prior to service for tripcocks, arrestors and SPAD control systems	0.02	3.09E+08	1.00E+06	3.08E+08	6.16E+06	6.16E+00	Preventive	Technical	T-16
		Emergency timetable - contingency plan for dealing with severe disruption (production of emergency timetables and dissemination of timetable information to all personnel especially operational personnel following an accident)	0.015	3.09E+08	2.00E+06	3.07E+08	4.61E+06	2.30E+00	Protective	Procedural	P-06
		Driver training - additional procedures to support drivers (SPAD)	0.02	3.09E+08	2.00E+06	3.07E+08	6.14E+06	3.07E+00	Preventive	Procedural	P-01E
		SPAD incident plan (immediate detection and action on signals passed at danger to reduce the consequence of failure)	0.05	3.09E+08	1.00E+06	3.08E+08	1.54E+07	1.54E+01	Dual	Procedural	P-07
		Crash worthiness and vehicle interior	0.3	3.09E+08	2.10E+07	2.88E+08	8.65E+07	4.12E+00	Protective	Design	D-07A
		ATC system introduction	0.9	3.09E+08	1.90E+08	1.19E+08	1.07E+08	5.65E-01	Preventive	Design	D-06B
		New/enhanced interlocking system - route locking system	0.9	3.09E+08	8.50E+07	2.24E+08	2.02E+08	2.37E+00	Preventive	Design	D-23
		Introduction of automatic signalling systems - minimisation of human error	0.9	3.09E+08	1.10E+08	1.99E+08	1.79E+08	1.63E+00	Preventive	Design	D-06A
		TPWS Train Protection and Warning System	0.7	3.09E+08	5.00E+07	2.59E+08	1.81E+08	3.63E+00	Preventive	Design	D-
		Signal overrun (Same as SPAD)		1.24E+08							
		Modify signalling to align with sighting constraints	0.8	1.24E+08	4.00E+07	8.37E+07	6.69E+07	1.67E+00	Preventive	Design	D-09B
		Speed restrictions (Adhesion)	0.6	1.24E+08	1.50E+07	1.09E+08	6.52E+07	4.35E+00	Protective	Operational	O-03D
		Additional testing and inspection of wheels and rail (NDT)	0.1	1.24E+08	6.00E+06	1.18E+08	1.18E+07	1.96E+00	Preventive	Technical	T-17
		Tripcock positions to be re-examined and potential relocation/re-installation	0.2	1.24E+08	5.00E+06	1.19E+08	2.37E+07	4.75E+00	Preventive		T-15

Major Accident	Contributors	Risk Reduction Options	% reduction achieved	Accident cost (£)	Cost (£)	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
		Exhaustive network survey to identify potential sighting issues	0.005	1.24E+08	3.00E+05	1.23E+08	6.17E+05	2.06E+00	Dual	Technical	T-18
	Emergency brakes fail to apply	*Extend overlaps*	0.4	4.95E+07	3.00E+06	4.65E+07	1.86E+07	6.20E+00	Preventive	Technical	T-11C
		Additional testing of brakes to determine if brakes are isolated	0.1	6.18E+07	1.00E+06	6.08E+07	6.08E+06	6.08E+00	Preventive	Technical	T-19
		Precautions, procedural modifications and subsequently, driver training for running with isolated emergency brakes	0.3	6.18E+07	3.00E+06	5.88E+07	1.77E+07	5.88E+00	Protective	Procedural	P-01F
		Introduction of enhanced braking system - eliminate scenarios where emergency brake signals fail to transmit to brakes (Same as 'improved braking' above)	0.95	6.18E+07	1.20E+07	4.98E+07	4.73E+07	3.95E+00	Preventive	Design	D-04B
		Assess the emergency brake performance of trains	0.05	6.18E+07	3.00E+05	6.15E+07	3.08E+06	1.03E+01	Dual	Technical	T-20
		Training for maintenance and test teams	0.1	6.18E+07	1.00E+06	6.08E+07	6.08E+06	6.08E+00	Preventive	Procedural	P-08
		Additional operational testing and inclusion in regime for rigorous asset acceptance/approval	0.15	6.18E+07	5.00E+06	5.68E+07	8.53E+06	1.71E+00	Preventive	Technical	T-21
	Delayed communications due to train radio system	*introduction of advanced radio/comms network across line section*	0.75	3.71E+07	1.10E+07	2.61E+07	1.96E+07	1.78E+00	Dual	Design	D-19A
		Rewiring/refurbishment of existing comms/radio systems	0.3	2.47E+07	1.10E+07	1.37E+07	4.12E+06	3.75E-01	Preventive	Design	D-20A
		Better communication between train drivers and line controllers - comms procedure/driver and line controller training	0.2	2.47E+07	6.00E+05	2.41E+07	4.83E+06	8.05E+00	Preventive	Operational	O-01B
		Update communication procedure and related procedures for drivers and line controllers	0.2	2.47E+07	6.00E+05	2.41E+07	4.83E+06	8.05E+00	Preventive	Procedural	P-09
	Traction power or track circuit of adjacent line not indicating occupied or showing	*Modify the train traction system e.g. filters, ICMU (Interference Current Monitoring Unit)*	0.1	6.18E+07	1.00E+06	6.08E+07	6.08E+06	6.08E+00	Preventive	Design	D-21

Major Accident	Contributors	Risk Reduction Options	% reduction achieved	Accident cost (£)	Cost (£)	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
	shorted by derailed train										
	Wrong direction train movement (due to 1. Signal Operator error and 2. Driver error)	*Extended overlap*	0.8	1.24E+07	3.00E+06	9.37E+06	7.49E+06	2.50E+00	Preventive	Technical	T-11D
	Collision with another train subsequent to a collision. [Both incident train drivers incapacitated (fast collision)]	*Emergency accident/incident plans*	0.3	2.47E+07	1.00E+06	2.37E+07	7.12E+06	7.12E+00	Protective	Procedural	P-10A
		Incident team on site - trained incident stations staff availability	0.4	2.47E+07	3.00E+06	2.17E+07	8.69E+06	2.90E+00	Dual	Operational	O-09
		Training for drivers and incident centre personnel	0.2	2.47E+07	1.20E+06	2.35E+07	4.71E+06	3.92E+00	Protective	Procedural	P-11
		Training for local emergency medical team on train accidents/incidents	0.2	2.47E+07	6.00E+05	2.41E+07	4.83E+06	8.05E+00	Protective	Procedural	P-12
		Additional procedures and subsequently, Driver and Signal Operator training - observation that wrong route is set prior to proceeding past signal	0.3	2.47E+07	1.00E+06	2.37E+07	7.12E+06	7.12E+00	Preventive	Procedural	P-01G
		Audible warning systems - trains	0.2	2.47E+07	1.10E+06	2.36E+07	4.73E+06	4.30E+00	Protective	Design	D-24A
		Points machine failure - new/enhanced point machines with 'route holding diversity'	0.75	2.47E+07	1.10E+07	1.37E+07	1.03E+07	9.36E-01	Preventive	Design	D-25A

APPENDIX A2: Risk reduction measures for Derailment accidents

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
Derailment	**Suspension failure (per train)**	*Replacement of rubber springs*							•								•												Dual
		Inspection and Maintenance of suspension to prevent incorrectly gauged suspensions in the depot prior to train deployment							•				•																Preventive
	Defective Wheel	*Improve inspection, testing and maintenance regime for detection of*							•				•																Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		wheel flat and worn wheel failures																											
		Additional training for route setting personnel						•	•				•		•														Preventive
	Excess speed - leading to derailment	*Speed restrictions*	•	•		•		•							•										•		•	•		Preventive
		Optimising cab design for driver protection in a collision							•		•	•			•										•		•	•		Preventive
		Traction/power assessment - introduction of systems such					•		•					•			•	•												Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		as surge arrestors, current limiters etc.																											
		Buffer stops															•		•											Protective
		Master controller installed in driver's cab for the driver to reduce or apply power to train					•		•																		•			Preventive
	Proceed under rule leading to derailment	*Review of operational concept/procedures for 'proceed-*						•	•																•	•				Dual

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		under-rule'																											
		Inspection and maintenance of shoe gear prior to deployment											•																Preventive
	Train falls down an embankment or from a bridge after a fast derailment	*Review programme for structural assessments/surveys - potentially more surveys/assessments introduced to existing programme*											•																Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		Structural re-inforcements - bridges, embankments							•																•		•	•		Protective
		Reduced traffic on bridge/structure										•							•					•						Protective
		Programme for assessment and management of workload for train drivers, line controllers, signallers and safety-critical staff							•						•									•						Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		Improve inspection and testing of fishplated joints - track							•				•																Preventive
		Replacement of fishplated joints							•	•			•																Preventive
	Tripcock fails to activate brakes	*Repositioning of tripcocks - standard requirement is tripcock positioning 1.5m from front of train*		•						•							•				•				•	•				Protective
		EMC studies on trains compatibility with				•			•					•													•			Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		track/signals - monitor interference levels, identification and introduction of relevant immunisation/ earthing solutions and potentially further operational railway testing																											
		Introduce training and competence management schemes for							•						•										•				Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		train crew																											
		Introduce injury prevention initiatives e.g. booklets, DVDs and staff briefings							•						•		•									•		•		Protective
		Review and improve rostering to reduce fatigue													•									•						Dual
		Unobstructed monitoring of drivers and train despatch and subsequent modifications to despatch						•	•						•												•			Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		rules (Rules for train despatch reviewed/simplified (procedural change and subsequently, driver training on new despatch rules)																											
		Improved management processes for train recovery							•						•											•		•		Preventive
	Loss of train detection - Train fails to shunt track circuit	*Introduction of sequential systems of various kinds such as axle*	•	•	•				•					•			•			•	•						•			Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		counters and other position detector systems etc. (in addition to track circuits to provide redundancy & diversity)																											
		Replacement of track circuits	•	•					•								•				•								Preventive
		Enhanced maintenance/testing such as detailed observation of the track circuit operation and								•			•																Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles													Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		re-adjustment of the track circuit (operating voltages)																											
		Introduction of (improved) shunting policy							•																•		•			Protective
		Review and improvement of recruitment and selection processes						•							•										•					Preventive
		Examining supervision and monitoring guidelines for operational safety staff,						•							•											•				Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		including shunters																											
		Trains fitted with incident response kits and additional training for staff to act as quickly as possible in emergency situations													•		•								•	•				Protective
	Involuntary exit	*Crowd control*															•											•		Protective
		Fire and rescue services													•		•							•	•	•		•		Protective

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		Paramedics/medical units (availability of staff trained for train accident scenarios)													•		•							•	•	•		•		Protective
		stronger windows -also minimises risk of object penetration through windows															•	•							•					Dual
	Emergency exit systems	*Emergency lighting and signage (illumination of Emergency Door Release*													•		•			•						•		•		Protective

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		mechanisms in passenger vehicles)																											
		Provision of hammers for emergency exit						•									•		•							•				Protective
	Track buckling & Side Swipe	*Track re-alignment to gauge (focus on track stressing & effects)*					•		•																				Preventive
		Track inspections - track vehicles											•		•														Preventive
		Track inspections - track workers											•		•														Preventive

Major Accident	Contributor	Risk Reduction Options	Preventive Risk Reduction Principles														Protective Risk Reduction Principles												Categorisation
			Built-in redundancy	Increased connectivity of systems or operations	Use of voting systems	Minimisation of sensitivity to single point failures	Derating	Simplifying operations	Reducing weak links in the design/operation	Maintaining continuity of action	Opposite effect modifications	Minimising Operations Frequency	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying rate of deterioration	Reducing Exposure time	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk planning, trouble shooting	Protective Barriers	
		Track refurbishment /renewals (including sleeper management programme to reduce gauge spread)							•																				Preventive
	Shoe caught under the conductor rail	*Track and conductor rail alignment*					•		•		•			•				•							•		•			Preventive

Major Accident	Contributors	Risk Reduction Options	Cost (£)	% Risk reduction achieved	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
Derailment	**Suspension failure (per train)**	*Replacement of rubber springs*	1.20E+06	0.05	4.59E+07	2.29E+06	1.91E+00	Dual	Design	D-26
		Inspection and Maintenance of suspension to prevent incorrectly gauged suspensions in the depot prior to train deployment	1.00E+06	0.1	4.61E+07	4.61E+06	4.61E+00	Preventive	Technical	T-39
	Defective Wheel	*Improve inspection, testing and maintenance regime for detection of wheel flat and worn wheel failures*	1.00E+06	0.1	4.61E+07	4.61E+06	4.61E+00	Preventive	Technical	T-40
		Additional training for route setting personnel	1.00E+06	0.1	4.61E+07	4.61E+06	4.61E+00	Preventive	Procedural	P-13
	Excess speed - leading to derailment	*Speed restrictions*	5.00E+06	0.8	1.83E+08	1.47E+08	2.93E+01	Preventive	Operational	O-10A
		Optimising cab design for driver protection in a collision	6.00E+06	0.3	1.82E+08	5.47E+07	9.12E+00	Preventive	Design	D-27
		Traction/power assessment - introduction of systems such as surge arrestors, current limiters etc.	1.00E+06	0.05	1.87E+08	9.37E+06	9.37E+00	Preventive	Technical	D-30A
		Buffer stops	5.20E+06	0.2	1.83E+08	3.66E+07	7.04E+00	Preventive	Design	D-39
		Master controller installed in driver's cab for the driver to reduce or apply power to train	6.00E+06	0.05	1.82E+08	9.12E+06	1.52E+00	Preventive	Design	D-28
	Proceed under rule leading to derailment	*Review of operational concept/procedures for 'proceed-under-rule'*	1.00E+06	0.05	1.78E+07	8.92E+05	8.92E-01	Preventive	Procedural	P-14
		Inspection and maintenance of shoe gear prior to deployment	1.00E+06	0.05	1.78E+07	8.92E+05	8.92E-01	Preventive	Technical	T-23
	Train falls down an embankment or from a bridge after a fast derailment	*Review programme for structural assessments/surveys - potentially more surveys/assessments introduced to existing programme*	1.00E+06	0.1	1.78E+07	1.78E+06	1.78E+00	Preventive	Procedural	P-15
		Structural reinforcements - bridges, embankments	1.50E+07	0.3	3.84E+06	1.15E+06	7.67E-02	Protective	Design	D-29
		Reduced traffic on bridge/structure	1.00E+07	0.5	8.84E+06	4.42E+06	4.42E-01	Protective	Operational	O-11
		Programme for assessment and management of workload for train drivers, line controllers, signallers and safety-critical staff	1.00E+06	0.1	1.78E+07	1.78E+06	1.78E+00	Preventive	Procedural	P-16
		Improve inspection and testing of fish-plated joints - track	1.00E+06	0.1	1.78E+07	1.78E+06	1.78E+00	Preventive	Technical	T-24
		Replacement of fish-plated joints	1.00E+07	0.3	8.84E+06	2.65E+06	2.65E-01	Preventive	Design	D-31
	Tripcock fails to activate brakes	*Repositioning of tripcocks - standard requirement is tripcock positioning 1.5m from front of train*	1.00E+06	0.3	9.32E+07	2.80E+07	2.80E+01	Protective	Technical	T-25

Major Accident	Contributors	Risk Reduction Options	Cost (£)	% Risk reduction achieved	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
		EMC studies on trains compatibility with track/signals - monitor interference levels, identification and introduction of relevant immunisation/earthing solutions and potentially further operational railway testing	6.00E+06	0.15	8.82E+07	1.32E+07	2.20E+00	Preventive	Technical	T-26
		Introduce training and competence management schemes for train crew	5.00E+06	0.08	8.92E+07	7.13E+06	1.43E+00	Preventive	Procedural	P-17
		Introduce injury prevention initiatives e.g. booklets, DVDs and staff briefings	2.00E+05	0.05	9.40E+07	4.70E+06	2.35E+01	Protective	Procedural	P-18
		Review and improve rostering to reduce fatigue	5.00E+05	0.15	9.37E+07	1.41E+07	2.81E+01	Dual	Procedural	P-19
		Un-obstructive monitoring of drivers and train despatch and subsequent modifications/amendments to despatch rules (Rules for train despatch reviewed/simplified (procedural change and subsequently, driver training on new despatch rules)	1.00E+06	0.1	9.32E+07	9.32E+06	9.32E+00	Preventive	Procedural	P-20
		Improved management processes for train recovery	1.00E+06	0.05	9.32E+07	4.66E+06	4.66E+00	Preventive	Procedural	P-21
	Loss of train detection - Train fails to shunt track circuit	*Introduction of sequential systems of various kinds such as axle counters and other position detector systems etc. (in addition to track circuits to provide redundancy & diversity)*	1.50E+07	0.3	1.26E+08	3.79E+07	2.53E+00	Preventive	Design	D-32
		Replacement of track circuits	5.50E+07	0.5	8.63E+07	4.31E+07	7.84E-01	Preventive	Design	D-33
		Enhanced maintenance/testing such as detailed observation of the track circuit operation and re-adjustment of the track circuit (operating voltages)	6.50E+06	0.1	1.35E+08	1.35E+07	2.07E+00	Preventive	Technical	T-27
		Introduction of (improved) shunting policy	1.00E+06	0.2	1.40E+08	2.81E+07	2.81E+01	Protective	Procedural	P-22
		Review and improvement of recruitment and selection processes	1.00E+06	0.1	1.40E+08	1.40E+07	1.40E+01	Preventive	Procedural	P-23
		Examining supervision and monitoring guidelines for operational safety staff, including shunters	1.00E+06	0.05	1.40E+08	7.01E+06	7.01E+00	Preventive	Procedural	P-24
		Trains fitted with incident response kits and additional training for staff to act as quickly as possible in emergency situations	4.00E+05	0.1	1.41E+08	1.41E+07	3.52E+01	Protective	Technical	T-28
	Involuntary exit	*Crowd control*	7.00E+06	0.2	8.72E+07	1.74E+07	2.49E+00	Protective	Operational	O-12A
		Fire and rescue services	5.00E+06	0.3	8.92E+07	2.68E+07	5.35E+00	Protective	Operational	O-13

Major Accident	Contributors	Risk Reduction Options	Cost (£)	% Risk reduction achieved	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Reduction/Cost	Categorisation	Option Type	Code (used for identification)
		Paramedics/medical units (availability of staff trained for train accident scenarios)	5.00E+06	0.3	8.92E+07	2.68E+07	5.35E+00	Protective	Operational	O-14
		stronger windows -also minimises risk of object penetration through windows	6.00E+06	0.4	8.82E+07	3.53E+07	5.88E+00	Dual	Design	D-35
	Emergency exit systems	*Emergency lighting and signage (illumination of Emergency Door Release mechanisms in passenger vehicles)*	2.00E+05	0.1	9.22E+06	9.22E+05	4.61E+00	Protective	Design	D-36
		Provision of hammers for emergency exit	1.00E+04	0.3	9.41E+06	2.82E+06	2.82E+02	Protective	Design	D-37
	Track buckling & Side Swipe	*Track re-alignment to gauge (focus on track stressing & effects)*	1.00E+07	0.8	2.25E+08	1.80E+08	1.80E+01	Preventive	Technical	D-14
		Track inspections - track vehicles	4.00E+06	0.75	2.31E+08	1.74E+08	4.34E+01	Preventive	Technical	T-xx
		Track inspections - track workers	2.00E+06	0.4	2.33E+08	9.34E+07	4.67E+01	Preventive	Technical	T-xx
		Track refurbishment/renewals (including sleeper management programme to reduce gauge spread)	2.50E+06	0.9	2.33E+08	2.10E+08	8.39E+01	Preventive	Technical	D-40A
	Shoe caught under the conductor rail	*Track and conductor rail alignment*	3.00E+06	0.8	4.41E+07	3.53E+07	1.18E+01	Preventive	Technical	T-29A

APPENDIX A3: Risk reduction measures for Platform Train Interface accidents

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
	Crowded platform inhibits driver's view (crowding)	*Additional support from platform supervisors*						•						•										•	•				Dual
		Audible warnings on platform (Improvements to passenger display screens and public address systems)						•						•										•	•	•			Protective
		Emergency plans - incident management plan												•										•	•				Protective
	Passenger falls from platform	*Programme of stair-nose marking*												•	•			•											Preventive
		Increased use of slip, trip and fall toolkit																		•				•					Protective

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Anti-suicide pits												•	•								•	•				•	Protective
	Passenger falls between cars	*Signage/Warnings and car door alarms (Trains)*					•	•						•				•	•				•	•		•			Protective
		Deployment of train co-ordinators train-cars						•						•									•	•					Dual
		Platform staff support (incident control - drag and pull) - Same as above Additional support from platform supervisors																						•	•				Protective
	Falls onto the platform from train	*Review of incidents of passengers being taken ill on trains to establish common causes*						•					•											•					Preventive

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		and develop plans to reduce the numbers of such incidents																											
		Gap fillers - Platform rubber												•				•				•							Protective
	Train passengers fail to activate Passenger Emergency Alarm (PEA) within station limits	*Introduction of Sensitive door system*		•			•	•										•	•				•						Protective
		PEA locations reviewed and relocated						•										•						•					Protective
		OPO CCTV (Same as 'Introduction of improved OPO CCTV systems' above)																					•						Protective
	Platform staff unable to stop train before it moves off with	*Additional support from platform supervisors (especially during*												•	•							•		•	•				Protective

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
	trapped customer	*rush hour or peak times) - Same as above Additional support from platform supervisors*																											
		Speed restrictions - enforcement of speed restriction on platform areas																					•		•				Protective
		Crowd control															•					•	•						Protective
		Additional platform lighting - Same as 'improve existing lighting' above												•	•									•	•				Dual
		Audible warnings on platform																						•	•	•			Protective

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures												Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
	Person pushed from platform	*Additional platform staff for supervision/control*																					•	•				Protective
	Person retrieving item from track	*Additional platform staff for supervision/control*																					•	•				Protective
		Under platform lighting						•						•								•	•					Dual
	Person on track due to self-action (miscellaneous)	*Audible warning systems - platform (station area) - Same as 'Audible warnings on platform…' above*																					•	•	•			Protective
		Audible warning systems - trains																					•	•	•			Protective
		Crowd control station platform area (Same as 'Crowd control')															•					•	•					Protective

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		above																											
		Speed restrictions - aerodynamic effect of train on passengers on platform (Same as 'Speed Restrictions - enforcement of speed restriction on platform areas' above)																					•		•				Protective
	Passenger strikes/falls against train	*OPO CCTV (Same as 'Introduction of improved OPO CCTV systems' above)*																					•						Protective
		Fencing						•			•				•			•					•						Preventive

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles													Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		Additional station area lighting												•									•	•					Protective
	Trespass on track in station area	*Audible warning systems - trains (See 'audible warning systems - trains' above*																						•	•	•			Protective
		Additional station/platform staff training (See 'Station Master/personnel training' above)																						•	•	•			Protective
		Closure of access to unused platforms or platform areas						•			•			•				•					•						Preventive
		Provision of staff at some locations, specifically to watch for people loitering on												•	•									•					Preventive

Major Accident	Contributors	*Risk Reduction Options*	Preventive Risk Reduction Principles												Protective Risk Reduction Measures													Categorisation
			Built-in redundancy	Increased connectivity of safety systems or operations	Use of voting systems	Derating	Simplifying systems or operations	Reducing weak links in the design or operation	Maintaining continuity of action	Opposite effect modifications	Minimising frequency of operations	Testing to precipitate latent faults	Minimise common cause failures	Minimise human errors	Separating hazards and triggers	Damage Arrestors	Reducing passenger vulnerability	Blocking pathways for escalation	Using fail-safe devices	Deliberately introducing weak links	Delaying the rate of deterioration	Reducing Exposure time/duration	Minimising the vulnerability of targets	Emergency systems and procedures	Processes/Systems in degraded conditions degraded conditions	Failure Indicators (failure status monitoring)	Prediction, Risk Planning, Trouble shooting	Protective Barriers	
		platforms																											

Major Accident	Contributors	*Risk Reduction Options*	Cost (£)	Risk Reduction Achieved	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Risk reduction/Cost	Categorisation	Option Type	Code (used for identification)
Platform Train Interface	Crowded platform inhibits driver's view (crowding)	*Additional support from platform supervisors*	5.00E+06	15%	1.29E+08	1.93E+07	3.86E+00	Protective	Operational	O-16A
		Audible warnings on platform (Improvements to passenger display screens and public address systems)	1.00E+06	10%	1.33E+08	1.33E+07	1.33E+01	Protective	Operational	O-18A
		Emergency plans - incident management plan	1.00E+06	10%	1.33E+08	1.33E+07	1.33E+01	Protective	Procedural	P-10B
	Passenger falls from platform	*Programme of stair-nose marking*	5.00E+05	8%	4.40E+07	3.52E+06	7.05E+00	Preventive	Technical	T-32
		Increased use of slip, trip and fall	1.00E+05	5%	4.44E+07	2.22E+06	2.22E+01	Protective	Technical	T-33

Major Accident	Contributors	*Risk Reduction Options*	Cost (£)	Risk Reduction Achieved	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Risk reduction/Cost	Categorisation	Option Type	Code (used for identification)
		toolkit								
		Signage/Warnings and car door alarms (Trains)	1.00E+06	10%	7.91E+06	7.91E+05	7.91E-01	Protective	Design	D-53
		Deployment of train co-ordinators train-cars	1.00E+06	5%	7.91E+06	3.95E+05	3.95E-01	Protective	Operational	O-21
		Platform staff support (incident control - drag and pull) - Same as above Additional support from platform supervisors	2.00E+06	20%	6.91E+06	1.38E+06	6.91E-01	Protective	Operational	O-16B
	Falls onto the platform from train	*Review of incidents of passengers being taken ill on trains to establish common causes and develop plans to reduce the numbers of such incidents*	5.00E+05	10%	1.78E+08	1.78E+07	3.55E+01	Protective	Technical	T-37
		Gap fillers - Platform rubber	2.00E+06	50%	1.76E+08	8.81E+07	4.40E+01	Protective	Design	D-55
	Train passengers fail to activate Passenger Emergency Alarm (PEA) within station limits	*PEA locations reviewed and relocated*	1.00E+06	20%	1.77E+08	3.54E+07	3.54E+01	Protective	Design	D-56
		Introduction of Sensitive door system	1.30E+06	30%	1.65E+07	4.95E+06	3.81E+00	Protective	Design	D-57
		OPO CCTV (Same as 'Introduction of improved OPO CCTV systems' above)	1.20E+07	80%	5.82E+06	4.65E+06	3.88E-01	Protective	Design	D-41B
	Platform staff unable to stop train before it moves off with trapped customer	*Additional support from platform supervisors (especially during rush hour or peak times) - Same as above Additional support from platform supervisors*	5.00E+06	40%	3.95E+07	1.58E+07	3.16E+00	Protective	Operational	O-16C
		Speed restrictions - enforcement of speed restriction on platform areas	5.00E+06	20%	3.95E+07	7.91E+06	1.58E+00	Protective	Operational	O-22A
		Crowd control	7.00E+06	20%	3.75E+07	7.51E+06	1.07E+00	Protective	Operational	O-12C
		Additional platform lighting - Same as 'improve existing lighting' above	5.50E+06	10%	3.90E+07	3.90E+06	7.10E-01	Preventive	Design	D-42B

Major Accident	Contributors	*Risk Reduction Options*	Cost (£)	Risk Reduction Achieved	Risk reduction (£) [Accident - Measure]	Actual Removed Risk (£)	Risk reduction/Cost	Categorisation	Option Type	Code (used for identification)
		Audible warnings on platform	1.00E+06	10%	4.35E+07	4.35E+06	4.35E+00	Protective	Design	D-58
	Person pushed from platform	*Additional platform staff for supervision/control*	5.00E+06	20%	3.95E+07	7.91E+06	1.58E+00	Protective	Operational	O-16D
	Person retrieving item from track	*Additional platform staff for supervision/control*	5.00E+06	10%	3.95E+07	3.95E+06	7.91E-01	Protective	Operational	O-16E
		Under-platform lighting	6.00E+05	10%	4.39E+07	4.39E+06	7.32E+00	Protective	Design	D-59
	Person on track due to self-action (miscellaneous)	*Audible warning systems - platform (station area) - Same as 'Audible warnings on platform…' above*	1.00E+06	10%	8.81E+07	8.81E+06	8.81E+00	Protective	Operational	O-18B
		Audible warning systems - trains	1.20E+06	10%	8.79E+07	8.79E+06	7.32E+00	Protective	Design	D-24B
		Crowd control station platform area (Same as 'Crowd control') above	7.00E+06	20%	8.21E+07	1.64E+07	2.35E+00	Protective	Operational	O-12D
		Speed restrictions - aerodynamic effect of train on passengers on platform (Same as 'Speed Restrictions - enforcement of speed restriction on platform areas' above)	5.00E+06	20%	8.41E+07	1.68E+07	3.36E+00	Protective	Operational	O-22B
	Passenger strikes/falls against train	*OPO CCTV (Same as 'Introduction of improved OPO CCTV systems' above)*	1.20E+07	40%	1.66E+08	6.65E+07	5.54E+00	Protective	Design	D-41C
		Fencing	3.00E+06	40%	1.75E+08	7.01E+07	2.34E+01	Preventive	Design	D-61
		Additional station area lighting	4.00E+05	10%	1.78E+08	1.78E+07	4.44E+01	Preventive	Design	D-62
	Trespass on track in station area	*Audible warning systems - trains (See 'audible warning systems - trains' above*	1.20E+06	10%	8.79E+07	8.79E+06	7.32E+00	Protective	Design	D-24C
		Additional station/platform staff training (See 'Station Master/personnel training' above)	1.00E+06	10%	8.81E+07	8.81E+06	8.81E+00	Protective	Procedural	P-25D
		Closure of access to unused platforms or platform areas	3.00E+06	40%	8.61E+07	3.44E+07	1.15E+01	Preventive	Technical	T-38
		Provision of staff at some locations, specifically to watch for people loitering on platforms	5.00E+06	10%	8.41E+07	8.41E+06	1.68E+00	Preventive	Operational	O-16F

APPENDIX B: Published Papers

APPENDIX B1: A new approach to risk reduction in the railway industry.

Institution of Engineering and Technology (IET) Special Interest Publication titled "The Infrastructure Risk and Resilience: Transportation", 47 – 52.

Abstract

In view of a number of fundamental weaknesses in the existing railway industry practice for selecting effective risk reduction measures, this paper proposes a new decision support approach based on sound, comprehensive and structured engineering principles from which risk reduction measures are identified. The proposed new approach is based on assessing the amount of risk the risks-reduction measures remove and their cost and on selecting the combination of risk-reduction measures which removes the largest amount of risk within the specified budget. We show that this approach is superior to the traditional cost-benefit-analysis approach, based on prioritising the risks according to their cost-benefit ratio and selecting only risk-reduction measures with benefit-cost ratio greater than one.

Keywords: Railways, Risk Reduction, Cost Effectiveness, Cost Benefit Analysis, Decision Support.

1. Introduction

Cost benefit studies are broadly used in the railways as a decision support tool for selecting accident reduction measures. A number of studies have exposed the inadequacies of the basic economic theories and practices in the transport industry [1].

Uncertainty in accident data has necessitated conservatism leading to an overestimation of the major accident risks on the railways. This paper presents a basic but structured approach to identifying and prioritising risk reduction measures for specific applications without reliance on accident risk data as currently practiced. The use of expected utility theory to reduce uncertainties associated with the application of cost-benefit analysis has been proposed in [2]. Attempts at developing alternatives to cost benefit analysis have also relied on economic theories. Currently, no practical and verifiable alternative exists for selecting risk reduction measures. Common sense suggests that the methodology must not be entirely dependent on historical accident data. A set of accident data is always associated with particular designs and conditions and cannot be transferred to new designs and new conditions. Accident frequencies relevant to old designs and conditions cannot be extrapolated to new designs and new conditions.

One of the primary requirements for risk reduction in the railway industry and similar safety-critical industries is that measures applied to reduce risks must be verifiable. This is a major challenge for the existing methods with their critical dependence on accident risk data. Sensitivity analysis has been considered as a tool for preventing misleading results from risk analysis and subsequently from cost-benefit studies. However, sensitivity analysis methods have been shown to contribute to inaccuracies, as a result of their limitations. These limitations have been well documented in [3-9].

2. Existing cost-benefit approach for risk-reduction

The choice of risk reduction measures is currently based on analysis using historical accident data with varying levels of uncertainty. As a result, the accuracy of decisions is often in question and could potentially lead to serious incidents. Figure 1 demonstrates the existing approach to reach decisions on risk reduction measures for investments on a typical railway project.

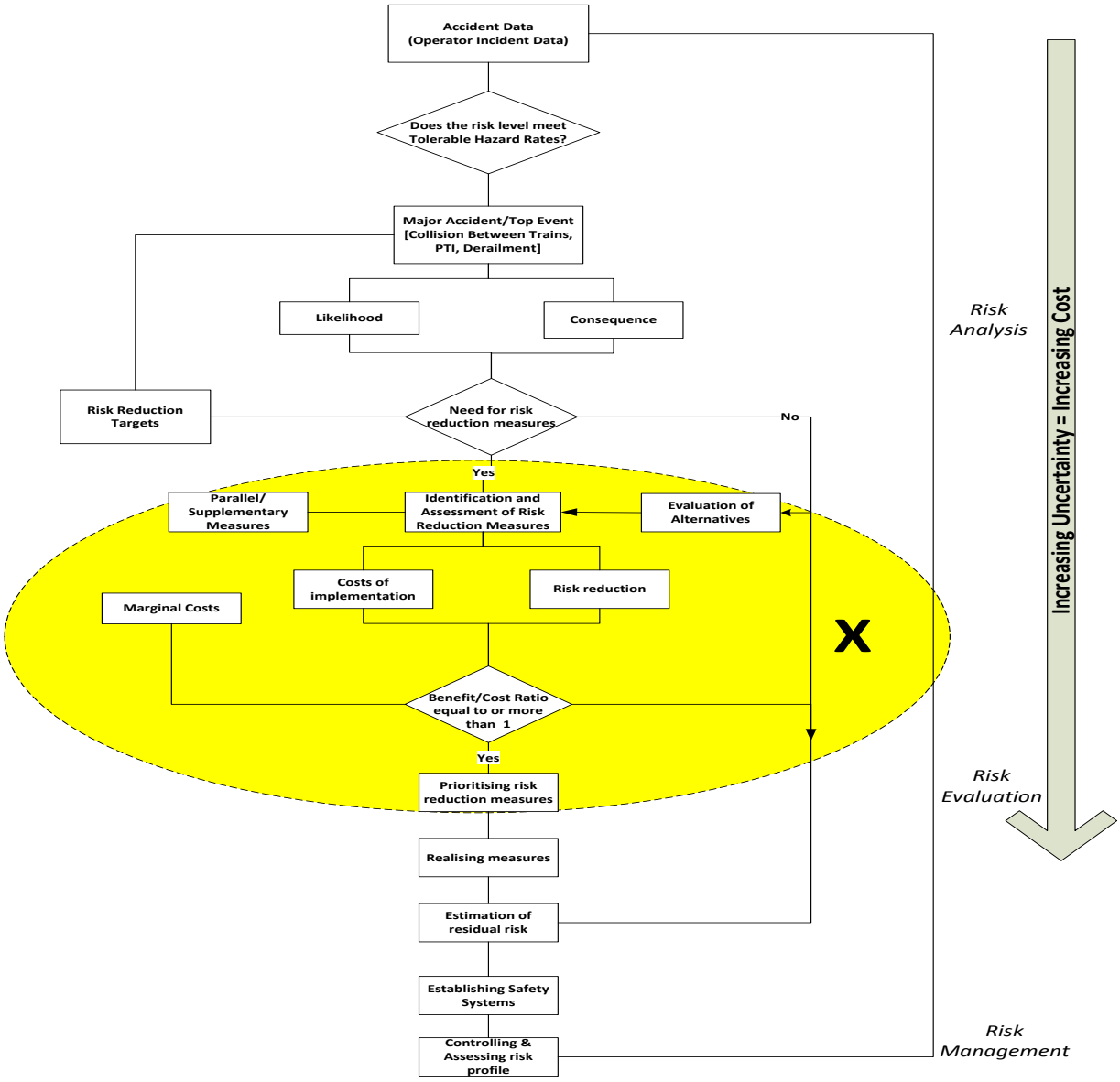


Figure 1: Existing cost-benefit approach for risk-reduction.

As can be seen from the diagram in Figure1, the cost-benefit approach to risk reduction is based on prioritising and selecting the risk reduction measures according to their benefit-cost ratio. Furthermore, despite the broad use of this approach, the effectiveness of the cost-benefit approach *cannot be verified as it is heavily reliant on historical data*. The historic data *are neither representative nor reliable for actual and estimated accident costs*. Furthermore, they are not valid to new designs and new conditions. These circumstances significantly increase ambiguity in decisions; reduce the level of confidence in the selected risk management procedures and make it impossible to develop a robust case for the railway safety application. This paper focuses on the highlighted region X in Figure 1 by introducing a well-defined and structured approach that replaces the highlighted activities. The proposed approach is based on the functional capability of the risk reduction measures applied to specific railway risk scenarios.

3. A new decision support methodology for selecting risk reduction measures

By using the cost-of-failure concept and the generic principles of risk reduction concept [10], an appropriated set of generic risk-reduction principles can be formulated, specific to the railway industry, from which risk-reduction measures can be derived. These risk-reduction measures reduce the likelihood of a railway accident or the consequence in the event of the accident. Subsequently, the identified risk-reduction measures are assessed with regards to the amount of risk each of them removes and the cost of their implementation. Table 1 presents 24 key generic principles for reducing risks in the railway industry. They are referred to as 'preventive' if they reduce the likelihood of a railway accident or 'protective' if they reduce the consequences, given that the accident has occurred.

Table 1: Key risk reduction principles (preventive and protective).

Principles for reducing the likelihood of an accident (Preventive)	Principles for reducing the consequence of an accident (Protective)
Built-in redundancy e.g. braking systems, route locking systems, position detection systems	**Protective barriers** e.g. thermal barriers as passive protective systems for risk reduction
Increased connectivity e.g. on-board train units.	**Delaying deterioration** e.g. refurbishments
Derating e.g. voltage alterations in track circuits for different operating temperatures	**Blocking pathways** through which accidents escalate e.g. platform emergency plungers
Reducing sensitivity to common cause failures e.g. design diversity in train control systems	**Introducing weak links** e.g. Crash Energy Management (CEM)
Minimising interfaces, complexities, weak links and connections e.g. use of closed communications networks	**Reducing the vulnerability of passengers** e.g. platform Closed Circuit Television (CCTV) or One Person Operated (OPO) CCTV for stuck at door or falls between train and platform
Simplification of operations e.g. use of software based systems to simplify application such as automating braking systems	**Use of fail-safe** devices in isolation techniques e.g. stick relays to de-energise track circuitry following an accident
Maintaining resistive forces and continuity of action e.g. wheel-slip and slide control	**Emergency response** e.g. emergency timetables, incident systems, first aid tool kit

Opposite effect modifications e.g. stressing track	**Degraded operations** e.g. speed restrictions
Operations frequency e.g. introducing trains into service to reduce overcrowding	**Damage arrestors e.g.** over-voltage or surge protection
Testing, inspections e.g. to detect latent faults	**Exposure time** e.g. crowd control
Reducing human errors e.g. training of drivers, controllers, in-cab designs.	**Failure indications** e.g. Automatic Warning System,
Voting systems reducing the likelihood of erroneous signals; interlocks preventing a wrong sequence of actions (e.g. controls and signalling systems)	**Prediction, risk planning and troubleshooting** e.g. use of leading and lagging indicators in risk reduction

The X-region in Figure 1 is replaced with a well-defined set of risk-reduction measures that provides the risk analyst and the decision-maker with a thorough and verifiable decision support system. Figure 2 presents the proposed decision support technique based on the 24 key risk reduction principles.

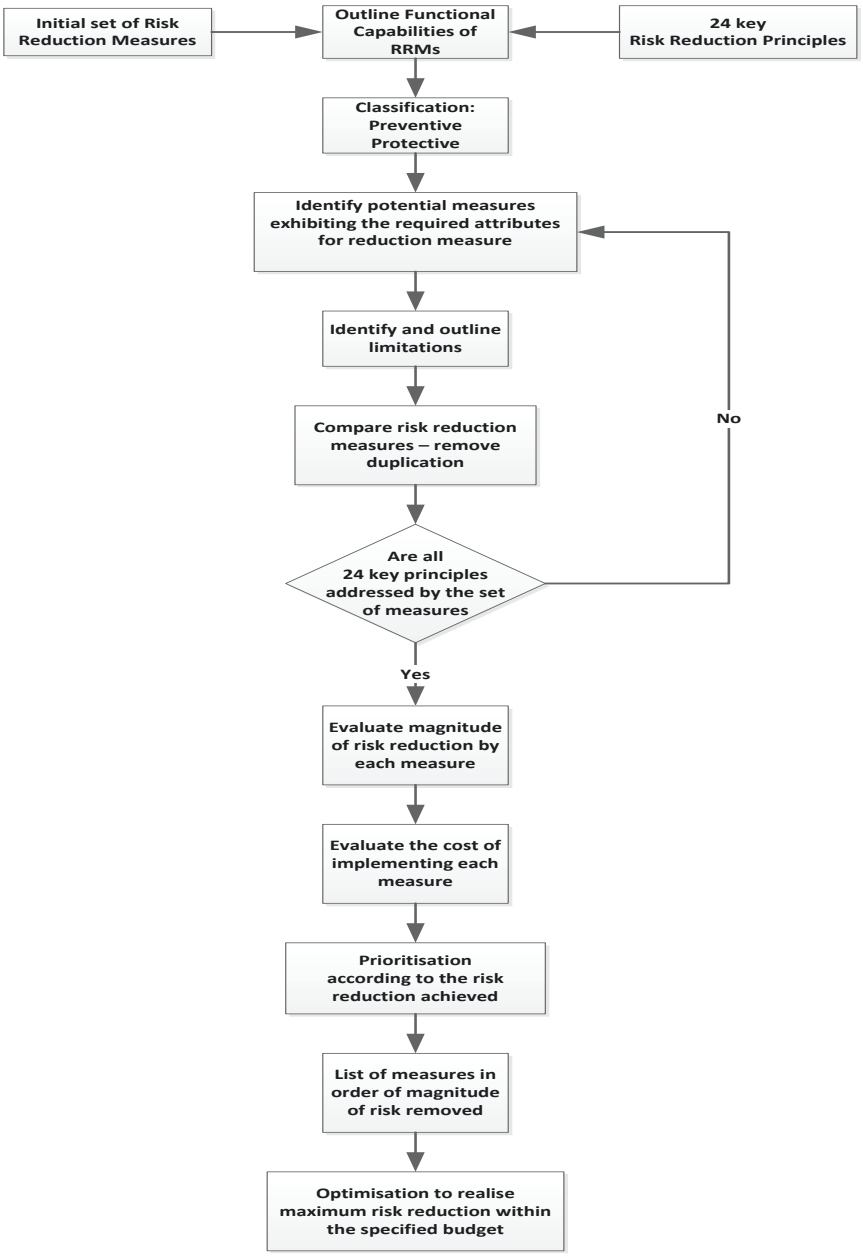


Figure 2: A simplified new approach

The process starts with assigning risk reduction measures to the different risk contributors or risk scenarios resulting in a major railway accident. Using the 24 key risk reduction principles, the measures are classified according to their potential for reducing the likelihood of the accident (preventive measures) or reducing the consequence given that the accident has occurred (protective measures). Each risk reduction measure is also assessed in terms of the magnitude of removed risk and its cost of implementation. A comparative analysis informs the decision maker of risk reduction measures with similar attributes.

4. Application of the decision support methodology for cost effective selection of risk reduction measures

The significant advantage of the proposed approach to the existing cost-benefit approach in selecting risk-reduction measures becomes clear from the following simple example. Suppose that a budget of £3 million has been allocated for the reduction of platform train accidents i.e. reduction in accidents involving passengers and trains at the platform area. This is a major risk which is located in the high-risk region of the risk matrix. The first risk reduction option 'A' requires the driver to operate a CCTV monitoring of the platform. The train will not be started if there are passengers stuck at the door, fallen onto the track or fallen between train and platform. Option B includes stop plungers - wall mounted alarm devices at specified locations/intervals within the platform area which can be operated by platform staff or passengers. Trains in the platform area will be brought to a halt by operating any of these plungers. Option C consists of gap fillers between train and platform to reduce accidents where passengers fall between train and platform whilst boarding the train. The three key risk reduction options, A, B and C have been evaluated, and the corresponding magnitudes of removed risk and costs are according to Table 2.

Table 2: Risk reduction measures with the associated costs and magnitude of the removed risk.

Risk Reduction Measure	Removed Risk [in millions £]	Cost of measure [in millions £]	Benefit/Cost ratio
A (One person operated CCTV)	2.0	1.60	1.25
B (Platform/passenger emergency stop plungers)	1.5	1.57	0.95
C (Gap Fillers)	1.2	1.3	0.92

To remove the major risk 'platform train accident' from the high-risk region of the risk matrix, risk of minimum magnitude £2.5 millions must be removed. If the cost-benefit approach is used, the first measure, A, with benefit-to-cost ratio greater than one, will be the only selected measure. Measures B and C will be ignored because their benefit- to-cost ratios are less than one. The magnitude of the removed risk within the specified budget is £2 million – insufficient to remove the major risk from the high-risk region of the risk matrix. In addition, the magnitude of the removed risk could be significantly larger, considering the specified budget of £3 million. According to the proposed new approach, options A and C should be selected, because this is the combination whose cost is still in the allocated budget of £3 million and the magnitude of the total removed risk is the largest. Furthermore, the magnitude of

removed risk according to the proposed approach will be £3.2 million, by 60% more than the amount of risk removed by using the cost-benefit approach. In addition, the amount of removed risk is sufficient to remove the major risk 'platform train accident' from the high-risk region of the risk matrix.

The next example is a real-life case, which has been an issue on all UK applications of the product 'axle counters', for over 10 years. The introduction of axle counters to achieve position detection for the trains, as a replacement for 'track circuits', is an illustration of the catastrophic effect of the cost-benefit approach which is based on historical data. Train position detection is a primary requirement for a safe operation of the railways. Due to lack of historical data regarding the frequency of failure of the axle counters, the accident history of the track circuit was used in the cost-benefit analysis. The cost-benefit analysis revealed net benefit of £500 per unit, from the use of axle counters. However, the historical data related to track circuits failed to reveal the following dangerous failure scenarios associated with the axle counters: (i) broken rails could easily be detected by the track circuit device but not by the axle counters; (ii) rail grinding wagons frequently brake axle counter heads, which makes them unsuitable for operation. These problems entail inability to detect broken tracks and, in addition, the axle counter heads have to be re-calibrated and re-installed after grinding operations. The result was increased risk levels to passengers, delays and severe operational challenges.

In this particular case, the use of the key risk reduction principles with the proposed systematic and iterative process would have identified the inherent flaws from the application of axle counters, thereby significantly reducing overall costs.

5. Conclusions

- The proposed decision support approach is a structured and comprehensive methodology for selecting risk reduction measures, where the likelihood of omitting a risk-reduction option is reduced to a minimum;
- The proposed decision support methodology is capable of identifying a set of risk reduction measures characterised by a larger removed risk within a specified budget, compared to the cost-benefit approach. The proposed methodology works particularly well in the common cases where the budgets for risk reduction are fixed and cannot be extended.
- The cost-benefit approach is based on historical accident data, which often results in a failure to detect dangerous new failure modes, if the technology or the operation conditions are changed.
- In contrast, the proposed decision support methodology does not depend on the completeness or correctness of historical accident data, which are often associated with great deal of uncertainty and have only local relevance.

- The decision support approach is an engineering application of sound risk reduction principles that support accurate classification of the risk reduction measures. Consequently, the proposed decision support approach provides confidence in the measures selected for risk reduction.

References

1. B. Flyvbjerg, M. Holm, K. Skamris, S.L. Buhl. “How common and how large are Cost Overruns in Transport Infrastructure Projects”, *Transport Reviews*, volume 23 (1): 71-88, (2003).
2. J. Li, S. Pollard, G. Kendall, E. Soane, G. Davies. “Optimising risk reduction: An expected utility approach for marginal risk reduction during regulatory decision making”. *Reliability Engineering and System Safety. Elsevier Ltd*, (2009).
3. A.C. Cullen, H.C. Frey. “Probabilistic Techniques in Exposure Assessment. A Handbook for Dealing with Variability and Uncertainty in Models and Inputs”. *Plenum, New York,* ISBN: 978-0-306-45957-3, (1999).
4. S. Menard. “Applied Logistic Regression Analysis”. *Sage Publications: Thousand Oaks, California*. ISBN 0-7619-2208-3, (1995).
5. D. von Winterfeldt, W. Edwards. “Decision Analysis and Behavioural Research”. *Cambridge, UK: Cambridge University Press,* pp. 399-405, (1986).
6. B.J. Winer, D.R. Brown, K.M. Michels “Statistical Principles in Experimental Design - Third Edition”. *McGraw-Hill Inc.*, (1991).
7. A. Saltelli, R. Bolado. “An Alternative Way to Compute Fourier Amplitude Sensitivity Test (FAST),” *Computational Statistics and Data Analysis*, 26(4), pp. 445-460, (1998).
8. H.R. Lindman. “Analysis of Variance in Complex Experimental Designs”. *W. H. Freeman & Co*, (1974).
9. J. Neter, M.H. Kutner, C.J. Nachtsheim, W. Wasserman. “Applied Linear Statistical Models - Fourth Edition”. *McGraw-Hill*. ISBN 978-0256117363, (1996).
10. M.T. Todinov. “Risk-based reliability analysis and generic principles for risk reduction”. *Elsevier*. ISBN 978-0080-44728-5, (2007)

APPENDIX B2: Optimal Risk Reduction in the Railway Industry by Using Dynamic Programming.

International Conference on Risk Safety and Security Engineering, World Academy of Science, Engineering and Technology 79, pp. 220 – 224.

***Abstract* —** The paper suggests for the first time the use of dynamic programming techniques for optimal risk reduction in the railway industry. It is shown that by using the concept '*amount of removed risk by a risk reduction option*', the problem related to optimal allocation of a fixed budget to achieve a maximum risk reduction in the railway industry can be reduced to an optimisation problem from dynamic programming. For *n* risk reduction options and size of the available risk reduction budget *B* (expressed as integer number),the worst-case running time of the proposed algorithm is O (n x (B+1)), which makes the proposed method a very efficient tool for solving the optimal risk reduction problem in the railway industry.

***Keywords* —** Optimisation, railway risk reduction, budget constraints, dynamic programming.

INTRODUCTION

THE railway operators and infrastructure owners are increasingly required to enhance services by introducing and implementing the best options for optimising risk reduction. In practice, the application of the "As Low As Reasonably Practicable" (ALARP) framework for risk reduction in the railway industry is a challenge, further compounded by decisions that must be made on a finite number of risk reduction options, within specified budgets. The current application of the cost-benefit technique as a decision support tool for determining the best options for risk reduction is inadequate 1 and there are advocates for alternative techniques 2. However, studies have exposed the inadequacies of applying basic economic theories in the transport industry 3. A fuzzy-analytical hierarchy process has been proposed by 4. The Analytical Hierarchy Process (AHP) requires the use of pair-wise comparison matrix and eigenvector to specify weights higher than a specified threshold 5, 6. AHP does not adequately support the decision-maker in choosing alternatives that have higher weights than the threshold and are unsuitable for selecting more than one choice when multiple alternatives are present 7. Other proponents of alternatives to the cost-benefit approach have demonstrated the application of different optimisation techniques in addressing risk reduction within budget constraints [8]–[15]. These studies apply multi-criteria methods such as AHP, *Simulated Annealing*, *Tabu Search*, *Genetic Algorithms*, *Expected Utility Theory* and combinations of these. The limitations of these approaches are well documented in [16]-[21]. A comprehensive analysis by 22, demonstrates that the optimal resource allocation problems are NP-hard problems. Studies undertaken on the suitability of optimisation techniques concluded that the optimal resource allocation is best addressed by using dynamic programming 23, [24].

In this paper, a case study of a railway line section has been used to demonstrate the effectiveness and accuracy of the dynamic programming optimisation technique for a major renewal project. The accident data set has been extracted from a 70km railway line with 34 stations, operating 33 - 35 trains daily. The railway line operates at an average speed of 60 to 70km/h line and 54 million journeys annually. The study focuses on the major accident risks on the line – Platform Train Interface (Platform-only accidents) and Collision between Trains. For the platform-only accidents, 20 available risk reduction options have been identified (Table I). The number of identified risk reduction options for the risk 'Collision Between Trains' was 81, of which only a small sample has been listed in Table II, due to space limitations. The risk reduction measures have been listed with the associated costs and risk reduction achieved.

TABLE I

A SET OF RISK REDUCTION OPTIONS FOR THE RISK OF PLATFORM TRAIN INCIDENTS (PLATFORM-ONLY)

ID	Risk Reduction Option	Cost [x £10,000]	Removed Risk [x £ 10,000]
1	Emergency/incident management systems	100	530
2	Station defect reporting & corrective system	10	35
3	Emergency drills – station staff training	20	67
4	Crowd control procedures & systems	100	265
5	Slip, trip, fall toolkit	10	20
6	Station surface inspections/testing/renewals	100	220
7	Platform Edge Doors (half length)	800	1360
8	Audible warnings on platform	100	132
9	Access & egress from incident site	200	260
10	Support from platform supervisors	300	320
11	Painted line warnings/signage	50	530
12	Platform emergency plungers – train stops	400	3900
13	Gap fillers	200	180
14	One-person-operated CCTV systems	1200	6100
15	Stair-nose marking	50	350
16	Station supervisor/personnel training	100	660
17	Re-design/r-build platform	1000	2800
18	Platform lighting (incl. emergency lighting)	550	1300
19	Increased traffic – major events, peak times	1000	1200
20	Enhanced surfaces –platforms	350	410

TABLE II

A REPRESENTATIVE SAMPLE SET FROM 81 RISK REDUCTION OPTIONS FOR THE RISK OF COLLISION BETWEEN TRAINS ACCIDENTS

ID	Risk Reduction Option	Cost [x £100,000]	Removed Risk [x £ 100,000]
1	Train stops	70	160
2	Speed restrictions – compromised overlaps	50	170
3	On-board sanding	20	60
4	In-cab CCTV	300	130
5	Driver training – Signal Passed at Danger	30	180

Algorithm for Solving the Problem of Optimal Budget Allocation in the Railway Industry

Let *S* be the set of all available *n* risk reduction options i=1,2,...,n, for a particular major risk in the railway industry. As a measure of the effectiveness of each risk reduction option, we postulate the measure *amount of removed risk*. The amount of removed risk is *the expected cost of prevented accidents, delays, fatalities, injuries etc. expressed in monetary terms*. Each risk reduction measure *i*, (i=1,2,...,n) is characterised by the amount of risk rr_i it removes after its implementation. Each risk reduction measure *i*, (i=1,2,...,n) is also characterised by its cost of implementation C_i.

Each risk reduction option cannot be selected more than once. As a result, each risk reduction option from the set *S* of all available risk reduction options can either be accepted or rejected.

The task of optimal allocation of the fixed budget reduces to determining the optimal subset $P \subseteq S$ of risk reduction options, whose total sum of removed risks $max \sum_{k\in P} rr_k$ is maximum and whose total cost of implementation does not exceed the available risk reduction budget *B*.

$$max \sum_{k\in P} rr_k; \sum_{k\in P} C_k \leq B \quad (1)$$

Considering the magnitude of the implementation costs for the risk reduction options in the railway industry and the magnitude of removed risks, it can be assumed that the costs and the amount of removed risk can always be expressed integer numbers. These express the removed risk and the cost of implementation in thousands, tens of thousands or hundreds of thousands of pounds sterling. It is also assumed that the available budget can also be specified by an integer number. As a result, the problem of optimal allocation of a risk reduction budget in the railway industry is reduced to a combinatorial optimisation problem involving integers only. This problem can be solved by using dynamic programming techniques 25, 26. Although the dynamic programming techniques have been known for a long time, to the best of our knowledge, in this paper, these methods have been applied for the first time to solve a problem of optimal risk reduction in the railway industry.

The advantage of the dynamic programming 23, 25, 26 consists of the fact that it finds solutions to sub-problems increasing in size, stores them in the memory and describes the solution of each sub-problem in terms of already solved and previously stored solutions of smaller sub-problems. As a result, sub-problems are solved only once, which makes the dynamic programming significantly more efficient than a brute-force method based on the enumeration of all possible subsets in the set of available risk reduction options *S*. The number of possible subsets in the set *S* is 2^n and the computational time of a brute-force method based on scanning all possible subsets increases dramatically with increasing the number *n* of risk reduction options.

The description of the algorithm in pseudo-code is presented next.

Algorithm 1: Building the Dynamic Risk Reduction Table

Initialising array x[][] with zeroes in the row with index '0' and in the column with index '0'.

```
for i=1 to n do
for  j=1 to B do
  {
cur_budget=j;
if (c[i]>cur_budget) then  { x[i][j]=x[i-1][j]; trac[i][j]=0; }
                    else
                    {
          rem = cur_budget-c[i];
tmp = rr[i]+x[i-1][rem];
if (x[i-1][cur_budget] >tmp) then {
x [i][j] = x[i-1][j]; trac [i][j]=0;
                                    }
else {
          x [i][j]=tmp; trac [i][j]=1;
             }
          }
  }
```

The algorithm works as follows. The solutions of the sub-problems are kept in the array x[][], where the rows correspond to the risk reduction options and the columns correspond to the available budget. The information necessary to restore the optimal solution is kept in the array trac[][]. The size of the x[][] array is (n+1) x (B+1) elements. The row with index '0' of the array x[][] corresponds to zero number of selected risk reduction options in the optimal set P; the column with index '0' of the array x[][] corresponds to zero budget.

The sub-problems are defined by the size of the current budget which varies from 1 to B units. The cost of the ith risk reduction option is compared with the value of the current budget and if it is greater than the current budget, the ith risk reduction option is not included in the optimal set *P*, which is reflected by placing zero in the trac array (trac[i][j]=0). In the case where the current budget is greater than the cost of the ith risk reduction option, a decision is taken whether to include the ith risk reduction option or not.

Initially, the statement 'rem = cur_budget-c[i];' determines the remaining budget if the ith risk reduction option is included in the optimal set P. The sub-problem marked by x[i-1][rem] however has already been solved and its solution has been recorded in the x[][] array. The entry x[i-1][rem] gives the maximum amount of removed risk within budget equal to 'rem' and for i-1 available risk reduction options.

Consequently, the solution of the sub-problem does not need to be determined again; it can simply be read out from the x[][] array. The amount of risk removed by the ith risk reduction option is rr[i]. Consequently, the maximum amount of removed risk for budget cur_budget=j,if the ith risk reduction option is included, is given by 'tmp = rr[i]+x[i-1][rem];'. If the ith option is not included in the optimal set *P,* the maximum amount of removed risk within the budget cur_budget is given by x[i-1][cur_budget], (cur_budget=j). Consequently, the decision whether to include the ith risk reduction option in the optimal set or not, depends on the outcome of the comparison made in the statement'if(x[i-1][cur_budget]>tmp)' where tmp = rr[i]+x[i-1][rem].

If 'x[i-1][cur_budget] >tmp', not including the ithrisk reduction option yields greater amount of removed risk and the entry'trac[i][j]=0'in the track[][] array is set to zero, which indicates that the ith risk reduction option has not been included in the optimum set of options P. The maximum amount of removed risk is equal to the maximum amount of removed risk within the current budget 'j', for i-1 total number of available options. This maximum however, has been computed and is already in the array x[][]; this is the entry x[i-1][j].

If 'x[i-1][cur_budget] <tmp', including the ith option yields greater amount of removed risk and the entry in the trac-array is set to one(trac[i][j]=1;), which indicates that the ith risk reduction option has been included in the optimal set P. The maximum amount of removed risk is equal to x[i][j]= rr[i]+x[i-1][rem].

In words, the maximum amount of removed risk is equal to the removed risk from including the ith risk-reduction option plus the maximum amount of removed risk for i-1 available options within the remaining budget 'rem'.

The optimal set of risk reduction options is restored by the next algorithm in pseudo-code.

Algorithm 2: Restoring the Optimal Set of Risk Reduction Options from the Dynamic Tables

```
Initialise all entries of the solution [] array with zeroes.
    cur_bud=B;
    cur_opt=n;
    tmp=trac[cur_opt][cur_bud];
    while (cur_opt> =1 ) do
                        {
    if (trac[cur_opt][cur_bud]=1)  then  {
    solution [cur_opt] = 1;
                                        cur_bud=cur_bud - c[cur_opt];
                                        cur_opt = cur_opt - 1;
                                                }
            else cur_opt=cur_opt-1;
```

}

The algorithm starts with the entry trac[n][B] of the track[][] array, which corresponds to a full budget *B* and all *n* available risk reduction options. If the n-th option has been included in the optimal set P, this will be indicated by a non-zero entry in the trac array (trac[n][B]=1). In this case, the solution array 'solution[]' marks the n-th option as 'included' in the optimal set P, by the statement 'solution [n]=1'. The current budget is then reduced by the statement 'cur_bud=cur_bud-c[cur_opt]' with the cost of the current (n-th) option. The current option to be considered should now be the n-1st option. This is ensured by the statement 'cur_opt=cur_opt-1'.

If the n-th option has not been included in the optimal set, this will be indicated by a zero entry in the trac-array (trac[n][B]=0). In this case, the current budget is not reduced because no cost has been incurred for implementing the n-th risk reduction option.

The process of considering the options in reverse order continues, until the first option is reached. At this point, the entries of the solution array will contain '1' for options which have been included in the optimal set P and '0' for options which have not been included in the optimal set P.

The running time of Algorithm 1building the dynamic table, is determined by the two nested loops: '**for** i=1 **to** n **do**' and '**for** j=1 **to** B **do**', which contain a set of operations that are executed in constant time. The maximum number of steps, after which Algorithm 1 will terminate, is $n \times B$. The maximum number of steps performed by Algorithm 2 is *n*, because after each iteration of the while-do loop, the number of options is reduced by 1. As a result, after at most *n* steps, Algorithm 2 will terminate. The total number of steps of the optimisation algorithm is therefore $\times B + n = n \times (B + 1)$. The worst-case running time of the algorithm for optimal allocation of a risk reduction budget is $(n \times (B + 1))$ . .

The algorithm has been tested on standard data sets with known solutions. For each of the data sets the algorithm returned the correct solution.

Now consider the risk 'platform train incident' with 20 available risk reduction options (Table I), whose removed risk and cost have been given as a multiple of £10000. For different specified budgets, the optimal set of risk reduction options are according to Table III.

TABLE III
OPTIMAL SETS OF RISK REDUCTION OPTIONS FOR THE RISK OF PLATFORM TRAIN INCIDENTS (PLATFORM-ONLY)

Budget [x £10,000]	**Optimal set of options**	**Cost of option [x £10,000]**	**Removed Risk [x £ 10,000]**
2900	1,11,12, 14,15,16,17	2900	14870
3300	1,4,6,9,11, 12,14,15,16,17	3300	15615
3500	1,2,3,5,11, 12,14,15,16,17,18	3490	16292
4000	1,2,3,4,5,6,8,9,11, 12,14,15,16,17,18	3990	17169

For the risk 'train collision' (Table II presents a representative sample data set) from 81 available risk reduction options, whose costs and associated removed risk have been given as a multiple of £100,000. For a specified budget of £110 million, the optimal set of risk reduction options is according to Table IV.

TABLE IV
OPTIMAL SETS OF RISK REDUCTION OPTIONS FOR THE RISK OF TRAIN COLLISION ACCIDENT

Budget [x £10,000]	**Optimal set of options**	**Cost of option [x £100,000]**	**Removed Risk [x £ 100,000]**
1100	1-3;5,6, 16,20, 26,30, 38,40-42, 44-46, 48-50, 53, 60, 62-66, 68, 69, 73-75, 77-80	1100	7446

The largest running time of the budget allocation algorithm, on a computer with processor *Intel(R) Core(TM) 2 Duo CPU T9900 @ 3.06 GHz*, was 0.015s!

Conclusions

1. By using the concept '*amount of removed risk by a risk reduction option*', the problem of optimal allocation of a fixed budget, among a finite number of risk reduction options in the railways industry, can be reduced to an optimisation problem from dynamic programming.
2. For a risk reduction budget *B* and *n* risk reduction options, the running time of the optimal allocation algorithm is O(*n* x (*B*+1)) (where *B* is the size of the budget).
3. The optimal solution for 81 available risk reduction options and various fixed budgets has been achieved within a very short time, which makes the developed algorithm a very efficient decision support tool for the railway industry.

References

1. Elvik, R. (2001). Cost–benefit analysis of road safety measures: applicability and controversies. Accident Analysis and Prevention. vol 33 (2001) pp. 9–17.
2. J. Li, S. Pollard, G. Kendall, E. Soane, G. Davies. "Optimising risk reduction: An expected utility approach for marginal risk reduction during regulatory decision-making". Reliability Engineering and System Safety. Elsevier Ltd, (2009).
3. B. Flyvbjerg, M. Holm, K. Skamris, S.L. Buhl. "How common and how large are Cost Overruns in Transport Infrastructure Projects", Transport Reviews, volume 23 (1): 71-88, (2003).
4. An M., Chen, Y., Baker, C. J. (2011). A fuzzy reasoning and fuzzy-analytical hierarchy process based approach to the process of railway risk information: A railway risk management system. Information Sciences 181 (2011) 3946–3966. Elsevier Inc.

5. Ramanathan, R., Ganesh, L. S. (1995). Using AHP for resource allocation problems. European. Journal of Operational Research, vol. 80, 417.
6. Saaty, T. (1988). The Analytic Hierarchy Process, McGraw-Hill, New York,
7. Ghazinoory, S., Aliahmadi A., Namdarzangeneh, S., Ghodsypour, S.H. (2007). “Using AHP and L.P. for choosing the best alternatives based the gap analysis”. Applied Mathematics and Computation vol. 184, pp. 316–321.
8. Rashid, M., Hayes, D. F. (2011). “Needs-based sewerage prioritization: Alternative to conventional cost-benefit analysis” Md. Journal of Environmental Management, vol. 92, 2427-2440. Elsevier Ltd
9. Cagno E., Di Giulio, A., Trucco, P. (2001). “An algorithm for the implementation of safety improvement programs”. Safety Science, vol. 37, pp. 59-75. Elsevier Science Ltd.
10. Persaud, B., Kazakov, A. (1994). “A procedure for allocating a safety improvement budget among treatment types”. Accident Analysis and Prevention. Vol. 26, No. 1, pp. 121-126. Pergamon Press Ltd.
11. Khisty, C.J., Mohammadi, J., (2001). Fundamentals of System Engineering, with Economics, Probability and Statistics. Prentice Hall, Inc., Upper Saddle River, N.J,pp. 1-57.
12. Lindhe, A., Rose´n, L., Norberg, T., Bergstedt, O., Pettersson, T.J.R. (2011). “Cost-effectiveness analysis of risk-reduction measures to reach water safety targets”. Water Research 45, pp. 241-253. Elsevier Ltd.
13. Ozkir, V., Demirel, T. (2012). A fuzzy assessment framework to select among transportation projects in Turkey. Expert Systems with Applications, vol. 39 pp. 74–80. Elsevier Ltd.
14. Sato, Y. (2012). “Optimal budget planning for investment in safety measures of a chemical company”. International Journal of Production Economics, vol. 140, pp. 579-585. Elsevier B.V.
15. Caputo, A. C., Pelagagge, P. M., Palumbo, M. (2011). Economic optimization of industrial safety measures using genetic algorithms.. Journal of Loss Prevention in the Process Industries, vol. 24 pp. 541-551. Elsevier Ltd.
16. Pirlot, M. (1996). “General local search methods”. European Journal of Operational Research, vol. 92, pp. 493-511.
17. Olson, D. L. (1988). “Opportunities and Limitations of AHP in Multi-objective Programming”. Math Computing Modelling, Vol. 11, pp. 206-209
18. Hey, J. D. (1995). “Experimental investigations of errors in decision making under risk”. European Economic Review, vol. 39, pp. 633-640. Elsevier Science B.V.
19. Van Laarhoven, P. J. M., Aarts, E. H. L., Lenstra, J.K. (1992). "Jobshop scheduling by simulated annealing". Operations Research, vol. 40, pp. 113-125.
20. Aven, T., Kørte, J. (2003). “On the use of risk and decision analysis to support decision-making”. Reliability Engineering and System Safety, vol. 79 pp. 289–299. Elsevier Science Ltd.

21. Fukuba, Y., Ito, K. (1984). “The so-called expected utility theory is inadequate”. Mathematical Social Sciences, vol. 7, pp.1-12. Elsevier Science Publishers B.V.
22. Basso, A., Peccati, L.A. (2001). “Optimal resource allocation with minimum activation levels and fixed costs – Theory and methodology”. European Journal of Operational Research, vol. 131 pp. 536-549
23. Horowitz, E., Sahni, S. (1974). "Computing partitions with applications to the Knapsack Problem", Journal of the ACM, vol.21 pp. 277-292.
24. Bjorndal, M.H. Caprara, A., Cowling, P.I., Croce, F.D., Lourenco, H., Malucelli, F., Orman, A. J., Pisinger, D., Rego, C., Salazar, J. J. (1995). “Some thoughts on combinatorial optimization”. European Journal of Operational Research, vol. 83, pp. 253-270.
25. Dasgupta, S., Papadimitriou, C., Vazirani, U. (2008). “Algorithms”. McGraw Hill, Boston, 2008.
26. Bellman R. (1957). “Dynamic programming”. Princeton, N. J., Princeton University Press.

APPENDIX B3: A new classification of risk-reduction options to improve the risk-reduction readiness of the railway industry.

International Journal of Systems Engineering, vol. 7, No. 9, pp. 816 – 825.

Abstract

The gap between the selection of risk-reduction options in the railway industry and the task of their effective implementation results in compromised safety and substantial losses. An effective risk management must necessarily integrate the evaluation phases with the implementation phase. This paper proposes an essential categorisation of risk reduction measures that best addresses a standard railway industry portfolio. By categorising the risk reduction options into *design, operational, procedural and technical options*, it is guaranteed that the efforts of the implementation facilitators (people, processes and supporting systems) are systematically harmonised. The classification is based on an integration of fundamental principles of risk reduction in the railway industry with the systems engineering approach.

The paper argues that the use of a similar classification approach is an attribute of organisations possessing a superior level of risk-reduction readiness. The integration of the proposed rational classification structure provides a solid ground for effective risk reduction.

[Keywords – systems, risk reduction, cost effectiveness, organisational readiness, railway]

1. Case for effectively implementing options for risk reduction

A considerable amount of effort is expended on planning, evaluation and management of potential risks prior to the selection of risk-reduction options. The selection of risk-reduction options would normally be preceded by a process of cost and benefit evaluation. In practice, the selection of risk-reduction options is constrained by fixed budgets. The greatest challenges of introducing and effectively managing risk-reduction options are the novelty of the option; the complexity of each risk reduction option; and the integration issues. The integration issues include (i) the interaction between subsystems to achieve risk reduction, (ii) the correlation and interaction among the risk reduction options and (iii) the correlation and interaction between the risk-reduction options and the environment. A comprehensive understanding of the limitations and strengths of each option for the specific application is a prerequisite for effective overall risk reduction. For major railway projects with multiple risk reduction options, the key to effective risk reduction lies in the successful integration of the available options. During the implementation phase, the integration of several options has the potential to expose an organisation to unanticipated problems and vulnerabilities. These problems are further compounded by an inefficient organisation.

This paper argues that a well-structured decision-support technique for selecting risk reduction measures must necessarily consider the organisational readiness to implement them, as an integral part of the risk options selection and evaluation. As a result, effective risk reduction during the "evaluation and selection" of risk-reduction measures benefits immensely from a systematic approach that considers the organisational readiness and structure.

There is surprisingly little research on the risks involved with the implementation of risk-reduction measures within the railway organization. Current studies, mostly organisation's internal risk management practices are limited in scope and cannot be generalised. In addition, there are no standard *measures of effectiveness* for the implementation of risk reduction options, not until an accident occurs. Most ALARP or risk management studies have been limited to identification, evaluation and options selection without any supporting analysis on the applicability of the selected options within the railway organization. Any knowledge in this area is hardly ever recorded and definitely not incorporated in in existing safety and business cases, despite the potentially severe financial and safety consequences. The existing safety and business cases do not analyse the risk reduction measures in relation to their mutual correlation, suitability and impact for the organisation. Without an organisational readiness to support effective implementation of the selected risk-reduction options, the existing safety and business cases are inadequate and weak.

2. Risk reduction on large-scale engineering projects

To address the potential challenges posed by the implementation of the risk reduction options on the railway industry, a thorough understanding of similar challenges from large-scale engineering projects is necessary.

As established by [1], hardly any publications exist on the effect that strategy, structure, processes and projects have on one another. The paper further argues that an integration of *strategy, structure, processes and projects* is required to facilitate the effective development of a business. In earlier work, [2] points to the *integration of organisational structure, control and prioritisation* as three critical areas necessary for effective risk reduction within large and complex engineering projects.

The key relationships between design, implementation and operational losses have been addressed in [3], [4] and [5]. [6] defines risk on large engineering projects as the possibility that events, their resulting impact and *dynamic interaction* may turn out differently than expected. The risk of project completion is further broken down to *technical, construction and operational* risks. A study on how design errors can severely jeopardise safety and contribute to failures in construction and engineering projects, with devastating economic, environmental and social consequences is presented by [7]. Design errors are

described as a symptom of dysfunctional organisational and managerial practices. [8] states that comprehensive product description and product requirements are essential influences on the risk patterns of IT organisations.

By comparing product architecture to organisational structure, [9] describe the failures in large-scale product development processes as a misalignment of the organisation to the product and points to two fundamental challenges: (i) the assignment of people to parts and subsystems that make up the product and (ii) the effective collaboration in the performance of design tasks. This is further supported by studies on railway organisation failures, primarily as a result of the misalignment between architectural/technical interdependence and organisational communication [10] – [13].

The risk of failure of large projects is a direct function of the level of interdependency among numerous parameters such as time, cost, scope, safety, environment, security and health. Within a project, the existence of interrelated risks, naturally results in triggering one risk from another risk and creating propagation phenomena such as reaction chains, amplification chains and loops. Using the network theory-based analysis, [14] proposed a risk reduction technique for reducing the risks of failure within large projects. The paper also states that the risk of failure is caused *by the lack of capacity to anticipate and control complex interactions*. [15] - [17] share the same view. However, [18] goes further by proposing that the key factors that drive complexity are project *size, variety, interdependence and context*.

The underpinning requirement for an effective organisation is that the organisation must successfully assimilate and implement technology and manage interactions between the source and the recipient of technology. *The capacity to efficiently act on knowledge is argued to be a critical activity that determines the readiness and value of an organisation's structure* [19]. To build on this point, it is important to note that any effort towards risk reduction must comprehensively consider the source of risk and the receiver, before any claims for effective risk reduction can be made. According to [20], the primary causes of failure for major engineering projects are: *the lack of understanding of users' and operational needs, poor staffing decisions, tight schedules and extensions to the functionality of an existing product without a comprehensive understanding of the technical challenges.*

The studies on the effectiveness of technology innovation, implementation and risk reduction have accumulated and advanced over a number of decades. The partitioning and interdependency of risks associated with the conceptualisation phase and the execution phase is best presented by [21]. Innovation is partitioned into an initiation phase and an implementation phase [22]. Within an organisation, high complexity, high diversity, low formalisation and low centralisation are most conducive

during the initiation phase, whilst low complexity, low diversity, high formalisation and high centralisation are most conducive at the implementation stage. In line with this theory, [23] demonstrate the potential constraints arising from inadequate specific knowledge of the project and the mutual self-reinforcing relationship between organisational structure and project. Later studies by [24] also pointed out that organisational structure, corporate culture and people are primary risks.

The risk of failure during implementation is three-dimensional in project size, experience with the technology and organisational structure. [25], [26] cite amongst other factors, the lack of organisational adaptation to complement technological change. An example of inappropriate applications is introducing new trains in small tunnels when it would have been easier to introduce advanced vehicle controllers only, at a cheaper price. Other important factors contributing to the risk of failure are the lack of skills to support implementation and the lack of exploration of a wide range of options.

These studies clearly indicate that the organisational structure is impacted by the risk reduction options selected and *vice versa*. Consequently, for effective risk reduction, it is mandatory to establish the relationship between risk reduction at the initiation stage (i.e. the stage of identifying and assessing risk reduction options) to risk reduction at the implementation (operational) stage where there is a significant contribution from the organisation and users. Fig. 1 illustrates that weaknesses in the implementation phase could partially or fully compromise the high-level of potential risk reduction achieved at the initiation stage. In order to achieve and maintain a maximum risk reduction, the organisation *must demonstrate readiness for acceptance and effective implementation of the risk reduction options identified at the initiation phase. These may include new techniques, technologies, processes etc*.

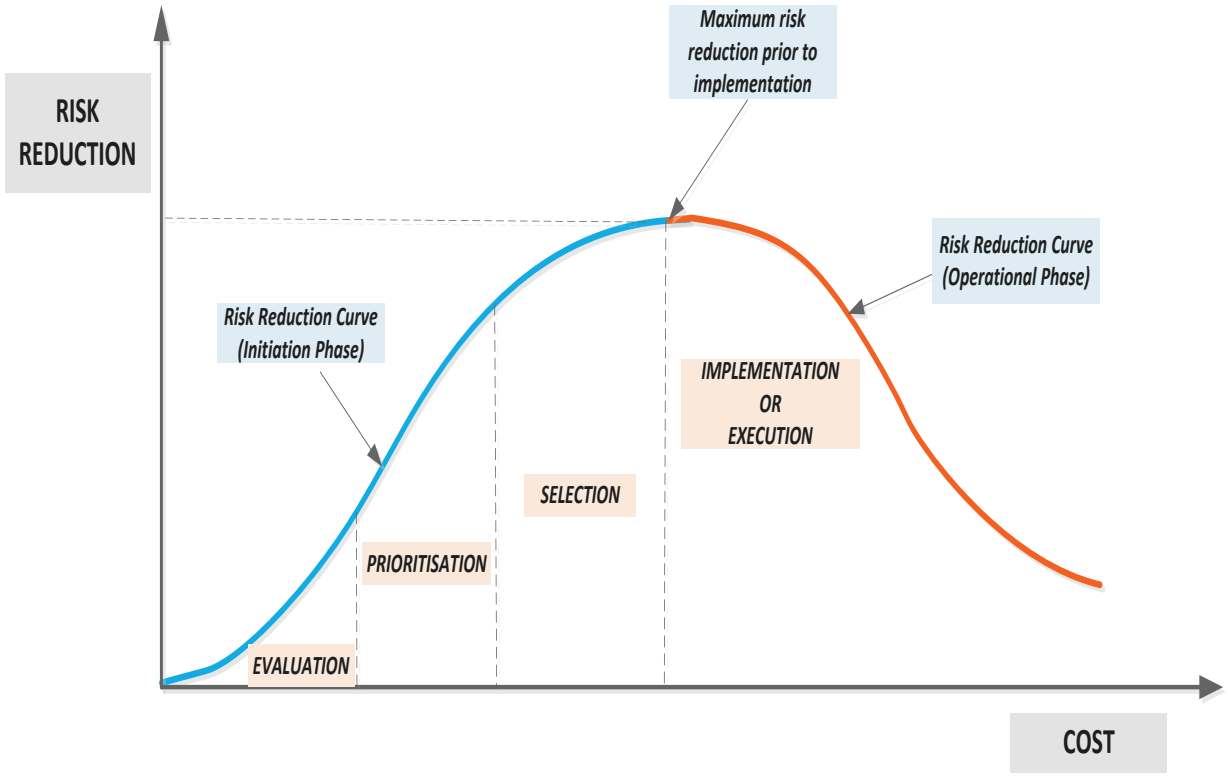


Figure 1: A risk Reduction Curve due to a poor implementation of the risk-reduction options selected at the initiation stage

3. Organisational readiness – complexities and management

Within an organisation that controls risks, ambiguous specifications and requirements for risk reduction, lack of clarity on the inter-relationships between risks, risk reduction options and the associated functions are major factors impacting effective risk-reduction. The issues related to managing multiple projects such as project prioritisation, selection and resource allocation in multi-functional organisations, are well defined in [27] - [30]. These issues are very similar to managing and implementing multiple risk reduction measures.

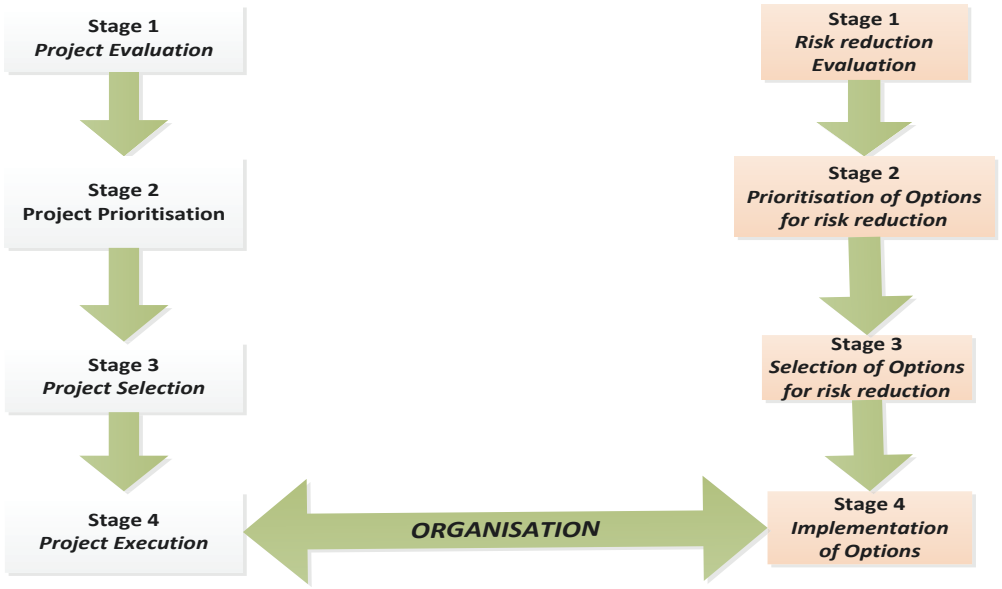


Figure 2: Parallelism between the implementation of **multi-functional projects** and the implementation of **risk reduction measures.**

The left-hand side of Figure 2 illustrates the key stages of effective management of projects. The essential stages in the implementation of risk reduction measures are provided in parallel (the right-hand side of Figure 2). The diagram clearly illustrates an existing parallelism between the two. The benefit from an improved organisational readiness has another, very important dimension - the capability to address unanticipated risks. Apart from operational circumstances that can be foreseen, there are also unforeseen risk events which are the product of unforeseen operational circumstances. These circumstances cannot be predicted, they are "unknown unknowns" or "black swans" [31]. We never know exactly what they are, but we do know they might occur. Improving the risk knowledge, the safety culture in the organisation and the level of general risk protection measures are effective barriers to unknown unknowns.

A change in the organisation structure may be necessary to effectively implement particular risk reduction options. This is for example the case when considering two options to eliminate wrong-side failures (i.e. failures leading to catastrophic consequences) for spring-applied parking brakes by (i) enhancing testing and maintenance regimes or (ii) by replacement with new braking systems. Selecting and implementing enhancing testing and maintenance regimes for example, requires specific organisation changes, (such as developing an organisation with emphasis on maintenance and testing rather than one with key expertise in design and manufacturing) if the measures are to result in maximising risk reduction. These organisational changes are driven not only by cost considerations. More importantly, these organisational changes are the only way to guarantee that effective risk reduction will be maintained through the life of

the operation. In common industry practice for selection of risk-reduction options, no publication, significant work or structured guide exists beyond the standard risk evaluation methods based on cost-benefit analysis (CBA). In fact, the existing approach does not consider the organisational structure (people, processes and tools/equipment) and its preparedness for the selection, evaluation and implementation of the risk reduction measures. The consequences of the lack of appropriate structure to support and maintain the maximum risk reduction are:

- Incorrect evaluation of risk-reduction options, which subsequently resulting in:
    - Reduced safety levels
    - Increased implementation costs
    - Inaccurate prioritisation of the risk reduction measures
    - Incorrect estimation of residual risks
    - Inaccurate risk profile
- Misalignment of selected risk-reduction options with the organisational capability and management structure, which leads to
    - Increased risk of failure to gain approval for the selected risk-reduction measures
    - Increased implementation costs
    - Inadequate implementation leading to degraded safety levels

Considering these consequences and existing practices, railway organisations typically have four distinct levels of readiness for implementing risk reduction. Table 1 presents the Risk-reduction readiness levels for railway organisations.

Table 1. Classification of railway organisations according to their level of Risk-Reduction Readiness.

Risk Reduction Readiness Levels	**Strategy**	**Description**
Level – 1	Reactive level	No risk reduction strategy. Reactive approach to risk management (dealing with risks as they materialise)
Level – 2	Basic level	Basic risk reduction based only on qualitative assessment and measures (e.g. by using risk matrix)

Risk Reduction Readiness Levels	Strategy	Description
Level – 3	Normative level	Risk reduction based on cost-benefit analysis which involves quantification of risk reduction options in terms of benefit and cost). No methodology for selecting risk-reduction options. No consideration of the interaction among risk reduction options. No optimisation in selecting the risk reduction options. No consideration of the impact of the selected options on the organisation and the environment. No consideration of the required organisational changes needed for the implementation of the selected options.
Level – 4	Optimal level	Risk reduction is based on a systematic approach impacting both the risk option selection, the precise quantification of removed risk and the optimal selection of risk reduction options. The impact of the selected options on the organisation and the environment is part of the analysis. The required organisational changes needed for the implementation of the selected options are carefully considered and specified.

Organisations at Levels 1 to 3 do not provide any support to maximising the risk reduction within fixed budgets. This increases the organisations' vulnerability to inaccurate assessments of risk and selecting weak and inefficient risk reduction options at escalating costs. The proposed classification, based on the fundamental principles of risk reduction and systems engineering is an initiative with the potential to provide a Level-4 framework that supports risk evaluation, optimal options selection and ultimately permits organisations to maximise risk reduction within fixed budgets. The proposed also bridges the gap between evaluation and selection of risk reduction options and specifying adequate organisational structure for their effective implementation.

4. Systems engineering approach to risk-reduction in a railway organisation

By definition, the system engineering approach to risk management must ensure effective risk reduction for any major railway renewal or developmental project.

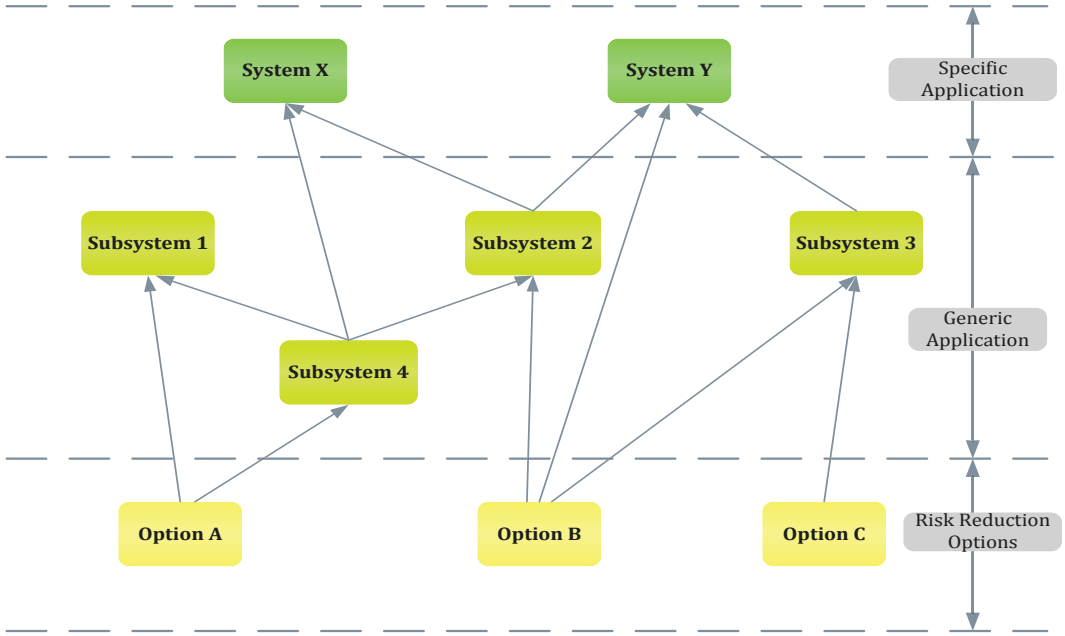


Figure 3. Systems engineering approach to risk reduction

During the initiation or concept phase, the risk reduction evaluation effort is determined by a complete and well-defined set of safety requirements. The specification of requirements must identify potential stakeholders. This ensures that the proposed solution is not only cost effective (i.e. feasible and affordable), but also guaranteeing the required levels of safety. On a large and complex project, the primary requirement for maximum risk reduction within a fixed budget is that the selection of risk reduction measures complies with the risk reduction potential and the budget constraints. This also requires a methodology that facilitates a comprehensive evaluation of the selected options. All operating modes (normal, degraded and abnormal) and the transitions between them should be considered. The way in which the systems will be operated, including the capacity and competence of personnel involved, operational arrangements and processes need to be fully understood in order to address the full set of possible operational scenarios. The integrated systems participating in the risk reduction exercise are a complex combination of people, processes and supporting structures (i.e. equipment or tools), whose interaction must be understood in order to achieve efficient risk reduction.

5. The inter-relationship between risk evaluation and risk reduction implementation

The introduction of new techniques, technologies or processes into the railways is usually associated with complexity and uncertainty. [32] qualify projects as *dynamically* or *structurally* complex and broadly dependent on project elements and interactions that are subject to change. This results in unpredictability, uncertainty and emergent behaviours. Structural complexities on the other hand, are quantifiable and predictable which provides an opportunity for better management. [33] provide insight

into the complexities and uncertainties involved in the risk reduction and effective management of large railway projects, in cases where there is predictability and in-built flexibility in the organisational structure.

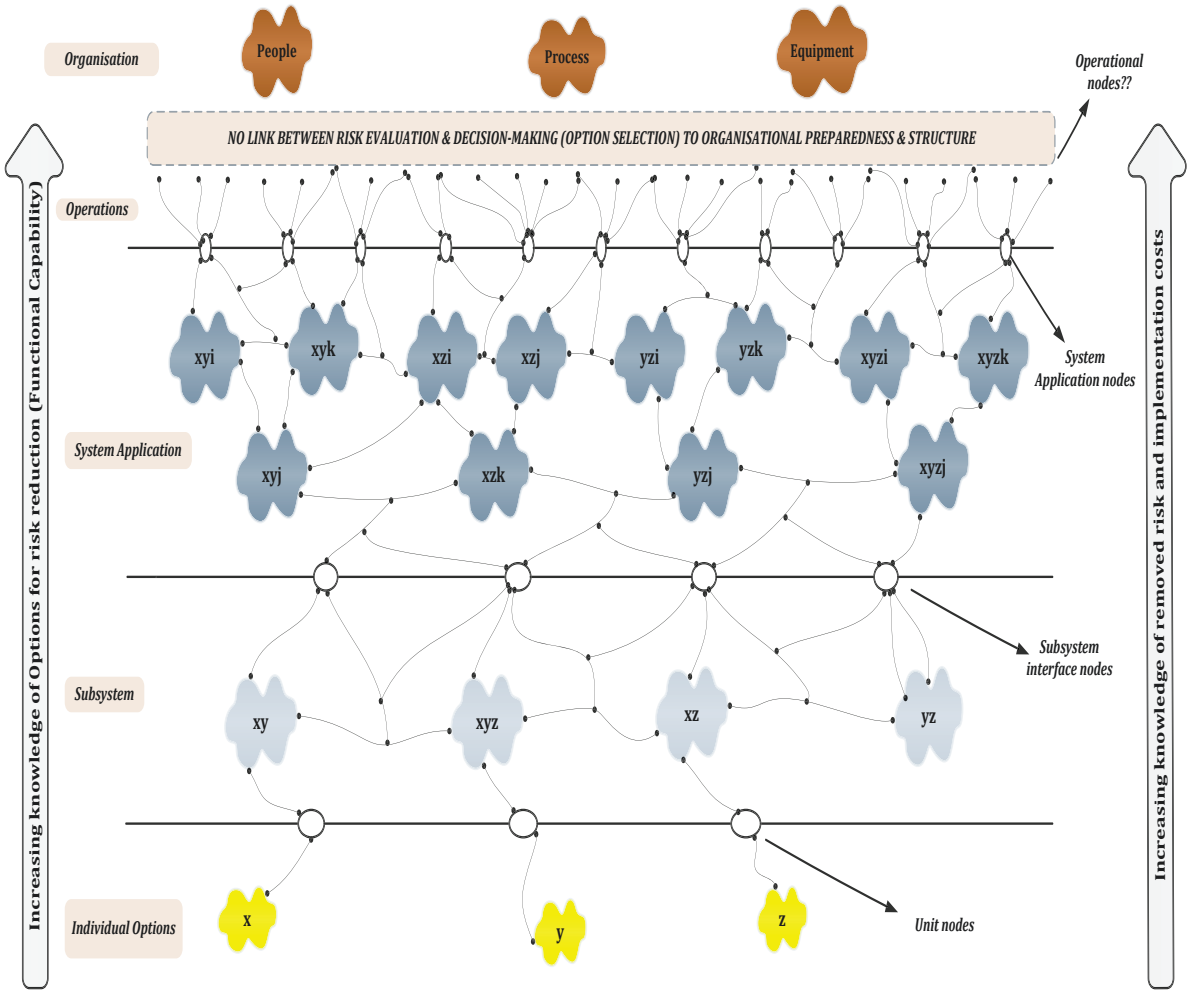


Figure 4. A system analysis is necessary for the effective implementation of the selected risk reduction options.

Figure 4 provides a simple illustration of the interactions and dependencies between risk reduction measures and the application environment which includes people, processes and equipment necessary for effective implementation. Figure 4 raises a fundamental question – is the railway organisation adequately built to facilitate the implementation of the selected risk-reduction options? In the current system, there is no link between the evaluation phase and the implementation phase of risk-reduction.

A simple practical illustration is the application of a number of risk reduction options to reduce the *Collision Between Trains* accident. The options are generally classed as (A) *brake assist systems*; (B) *collision warning systems* and (C) *intelligent speed adaptation systems*. Options A, B and C achieve the risk reduction because of their inherent operational characteristics. In practice, these options are not

mutually exclusive and an investment in all options (A, B and C) is often required to achieve effective risk reduction. While for risk reduction options which are relatively independent, the application of dynamic programming techniques is fully justifiable and leads to a significant risk reduction within a fixed budget [34], additional (systems) analysis is needed for correlated risk reduction options. In cases where some of the options are incompatible (cannot be applied simultaneously) or in cases where the effective risk reduction from the application of one option requires the application of another option, the blind application of standard optimisation tools may not result in the expected risk reduction.

The limitations, the required conditions and existing interactions among the risk-reduction options should be thoroughly understood and accurately specified.

Additional risk reduction options, typically introduced in railway safety to reduce the Collision Between Trains accidents include: extension of signals, train movement rules, incident response systems, train driver training, speed restrictions, wheel-slide protection systems, In-cab design modifications, operational testing and maintenance, emergency timetables, track inspections and refurbishment, one-person (driver) operated closed circuit television, etc.

Following this understanding, a number of additional measures can be combined with the selected options A, B and C to achieve a significant risk reduction:

Option A: Brake assist system + (operational testing and maintenance, train driver training, one person-operated closed circuit television)

Option B: Collision warning systems + (train driver training, in-cab design modifications, speed restrictions, emergency timetables)

Option C: Intelligent speed adaptation + (Train movement rules, wheel-slide protection, extension of signals, emergency timetables)

For example, investing in brake assist systems (Option A) without investing in operational testing and maintenance does not permit obtaining a long term risk-reduction benefit from investing in expensive brake assist systems. Risk reduction Option A requires also investing in testing and maintenance if a long-term risk-reduction effect is to be achieved.

Similarly, investing solely in collision warning systems (Option B) without simultaneously investing in driver education and training does not permit obtaining the risk reduction benefit from applying solely Option B. As a result, if Option B is to have a tangible risk-reduction effect, investment in another risk reduction option (“driver training and education”) is required. In fact, without driver training and

education, there may not be any risk reduction benefit from purchasing expensive collision warning systems.

By considering these interactions as important factors in the risk reduction exercise, the safety and business case claims for risk removed and cost effectiveness can be justified and further enhanced to support their acceptance and successful implementation.

By revealing the complex interrelations among the risk reduction options, the gap between risk evaluation, options selection and implementation (i.e. costs, people, process and equipment) can be effectively closed. The adoption of the systems approach provides coordination between people, processes and equipment at the implementation phase, where the organisation plays a crucial role in the risk management process. In this sense, the systems approach provides a bridge to the organisation structure.

6. A new classification of risk-reduction options

As established, integrating risk evaluation with the primary operational functions is a fundamental requirement for successfully making the case for the selected options. This requirement is especially applicable to industries where risk management drives investments and decisions. [36] and [37] expound on the topic related to effective management of operational risks. These risks are defined as event risks and to effectively handle the risks of potential losses, categorisation of events is necessary. This serves as a receptacle for accident data gathering on frequencies and costs. A tentative categorisation for managing potential operational losses is further provided as People, Processes, and Systems.

The Railways and Other Guided Transport Systems (Safety) Regulations 2006 [38] requires that the infrastructure operator and maintainer of the railways demonstrate how safety risks will effectively be managed and whether the infrastructure operator and maintainer have the ability, commitment and resources to comply with the regulations. This is generally addressed by *(i) demonstrating capability, commitment and availability of resources to manage safety risks; (ii) the safety case which provides a framework against which regular assessments, risk control measures and management systems are established and maintained (ii) the safety case assures regulators that the risks associated with operations have been assessed and all reasonably practicable controls have been implemented to reduce the risks.*

The areas that are considered safety-critical and have a direct impact on the successful prevention of accidents on the railways are typically *signalling and train control (communication systems); train driving and train operations; train manufacture, maintenance and refurbishment; installation, renewal and maintenance, faulting and inspection of infrastructure; safety of passengers on trains; passenger and*

visitor movement on stations and platforms; on-track machine manufacture, maintenance and refurbishment. The major accidents that are to be reduced are attributed to *risk of derailment*, *risk of collision between trains* and *risks related to the passenger train interface*.

Following the argument that effective risk management must necessarily integrate the initiation (evaluation) phase with the implementation phase, we propose a categorisation of risk reduction measures that best addresses a standard railway industry portfolio. The introduction of a structured approach based on categorising the options for reducing major accidents, reflects the standard railway organisational structure. By categorising the risk reduction options into *design, operational, procedural and technical options*, it is guaranteed that the efforts of the implementation facilitators (people, processes and supporting systems) are systematically harmonised. The categorisation effectively simplifies a complex register of risk reduction options and combination of options into a format that reflects the typical railway organisational structure and helps reduce the gap between the evaluation and implementation phase.

The categorisation includes:

- *Design risk-reduction options (DRRO)* – Novel systems, major renewals and modifications
- *Operational risk-reduction options (ORRO)* – Communications, Supervision and Speed Restrictions or similar operational decisions
- *Technical risk-reduction options (TRRO)* – Testing, Maintenance, Inspections, Installations, Assessments/Studies informing risk reduction decisions
- *Procedural risk-reduction options (PRRO)* – Risk education, Risk training, Processes and Plans

Each risk reduction option, within each group, is based on sound engineering principles for risk reduction. The effectiveness of each of these options has been proved by theoretical considerations, reliability and risk modelling, field testing and historical track records. The introduction of these options reduces the complexity of selecting risk reduction options for different applications. At the same time, the classification guarantees that no efficient risk-reduction option is missed at the evaluation phase. Consequently, this classification will be particularly useful for major railway projects with numerous possible risk reduction options, typically reflecting all aspects of the standard railway organisational operations including: *design*, *maintenance*, *testing, new technologies* etc. *combined with people*, *processes and equipment*. Table 2 presents a structured categorisation that supports the option selection and the evaluation of individual options and combination of options. The systematic process of categorising the risk reduction options and aligning them with the existing organisational functions also supports the identification and assignment of responsibilities for effective implementation. Table 2 and

Figure 5 also illustrate the relationship between the major accident hazards, risk reduction measures and the direct link with the organisational instruments – people, process and equipment. Figure 5 also depicts the role of the proposed categorisation in the relationship between these, for effective risk reduction.

Table 2. Categorisation of risk-reduction options in the railway industry.

RISK REDUCTION OPTIONS	EXAMPLES OF RISK REDUCTION OPTIONS	Key Function(s) for implementation
DESIGN OPTIONS (DRRO) **Novel Systems, Major Renewals, Design Modifications (Capital Intensive Projects)**	1. Signalling replacements and modifications - automatic signalling and control systems 2. Optimising cab design for driver protection	Chief Engineer, System Integration, Programme Directorate, Project Management
TECHNICAL OPTIONS (TRRO) **Testing, Maintenance, Inspections, Installations, Assessments/Studies**	1. Improving inspection, testing and maintenance regime for detection of wheel flat and worn wheels 2. Signal positioning studies and potential extension of distances between signals	Technical Assurance, Civil and Power Engineering, Signalling Systems Engineering, Train Systems Engineering, Asset Management
PROCEDURAL OPTIONS (PRRO) **Risk education and training, Processes and Plans.**	1. Risk education and training of key personnel 2. Amendments to train despatch rules 3. Review and improvement of recruitment and selection processes	Infrastructure and Systems Protection, Training Management or Organisational Development.
OPERATIONAL OPTIONS (ORRO) **Communications, Supervision and Speed restrictions**	1. Crowd Control 2. Speed restrictions (adhesion)	Operational Engineering, Telecommunications Systems Engineering

The clear outline of the roles and responsibilities within the risk reduction exercise ensures that resources such as finances, technical expertise, information, systems and equipment, medical facilities etc., necessary for implementing the measures are available and appropriately targeted. In the risk reduction effort, undertaking emergency and preparedness planning, immediate post-accident actions and response is absolutely essential. The inter-relationships between departments, participating in the risk reduction operation, can be used for developing measured strategies for accident prevention and

protection. Throughout the project lifecycle, the clearly defined inter-relationships between departments ensure that the railway operations also make it possible to take advantage of the many technical resources that already exist within the organisation. By reflecting the typical railway organisational structure, the proposed categorisation makes it possible to tap into the existing resources within the organisation.

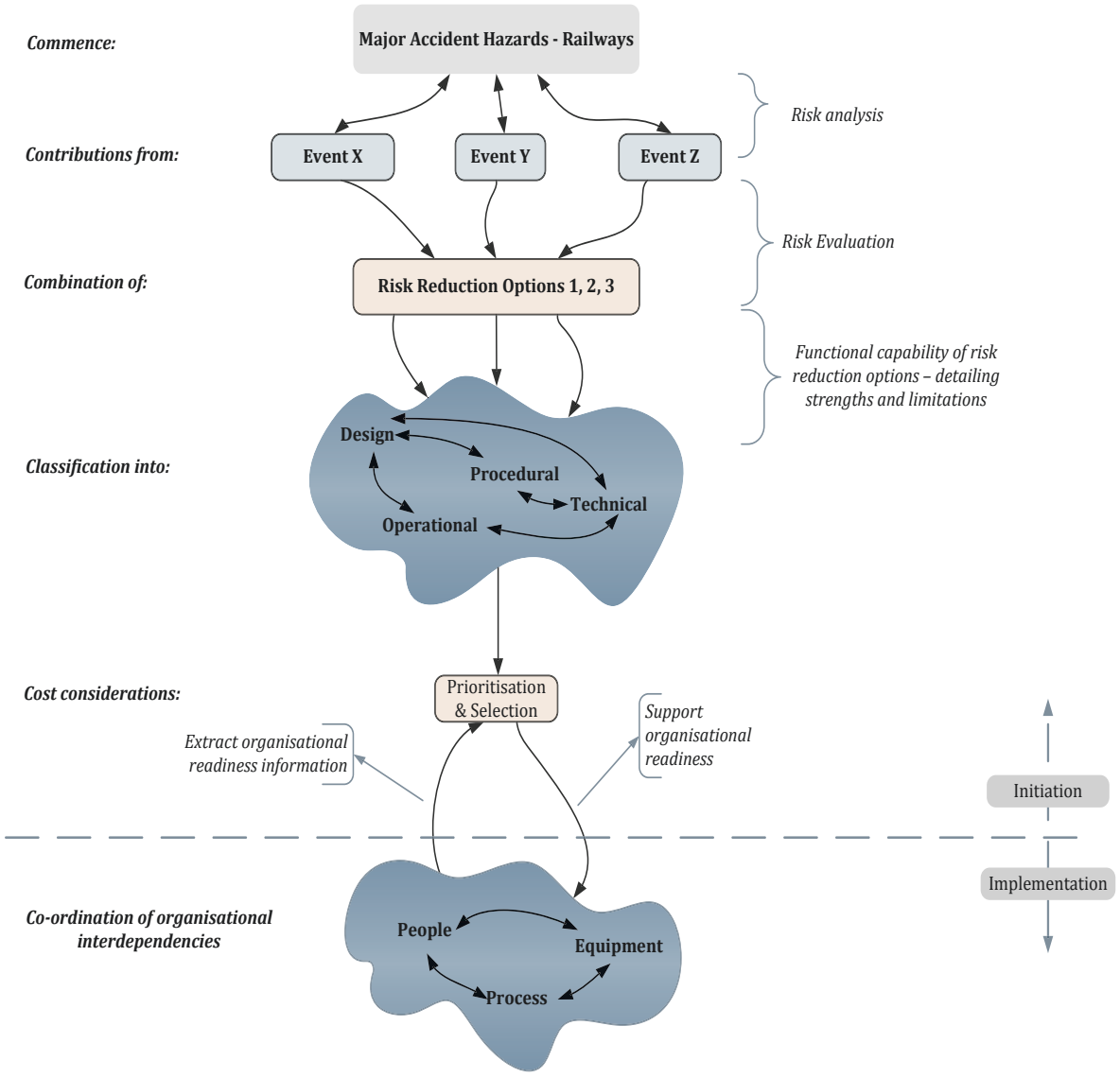


Figure 5: Categorisation of risk-reduction options, risk management and the organisation

The proposed classification promotes a comprehensive understanding of the risks resulting in an accident and provides a strong support to the *Lessons learned database*. It provides a direct and strong support to the comprehensive check lists related to known accident scenarios which is an important tool for identifying possible accident and failure scenarios. The proposed methodology also draws on concepts from organisational theory and optimization of risk reduction as introduced by [38]. However, by considering the intricate interrelations between risk reduction options and the organisational

interdependences, it goes beyond the development in [38] and promotes a novel framework that bridges the divide between the identification and implementation of risk reduction measures within railway organisations.

7. Readiness for effective risk reduction

A significant amount of effort towards risk reduction in the railway industry is associated with major renewal projects. The renewal projects are usually large-scale engineering undertakings which provide the railways with necessary modifications and improvements. Along with reducing particular risks, these projects introduce new risks to railway operations. Consequently, essential risk reduction measures are considered and implemented to ensure that the safety integrity of the railways is not compromised, and where possible, improved. The new risks are the result from altering fundamental operational parameters such as *increasing number of trains to cater for a greater passenger volume* or *the removal of speed limits to meet operational schedules*. The situation is complicated considering that these changes are weather-dependent – they are different during different times of the year. The challenges facing the railway industry are the unrelenting pressures to reduce cost, improvements for customers and pressure to maximise the use of the asset base.

However, the organisational changes and modifications, every time a big renovation project is initiated are very costly. A railway organisation that has not taken the necessary steps to a dynamic and flexible organisation in relation to risk reduction, easily incurs significant implementation costs. The significant increase in implementation costs usually deters the selection of appropriate risk reduction options to achieve a maximum risk reduction.

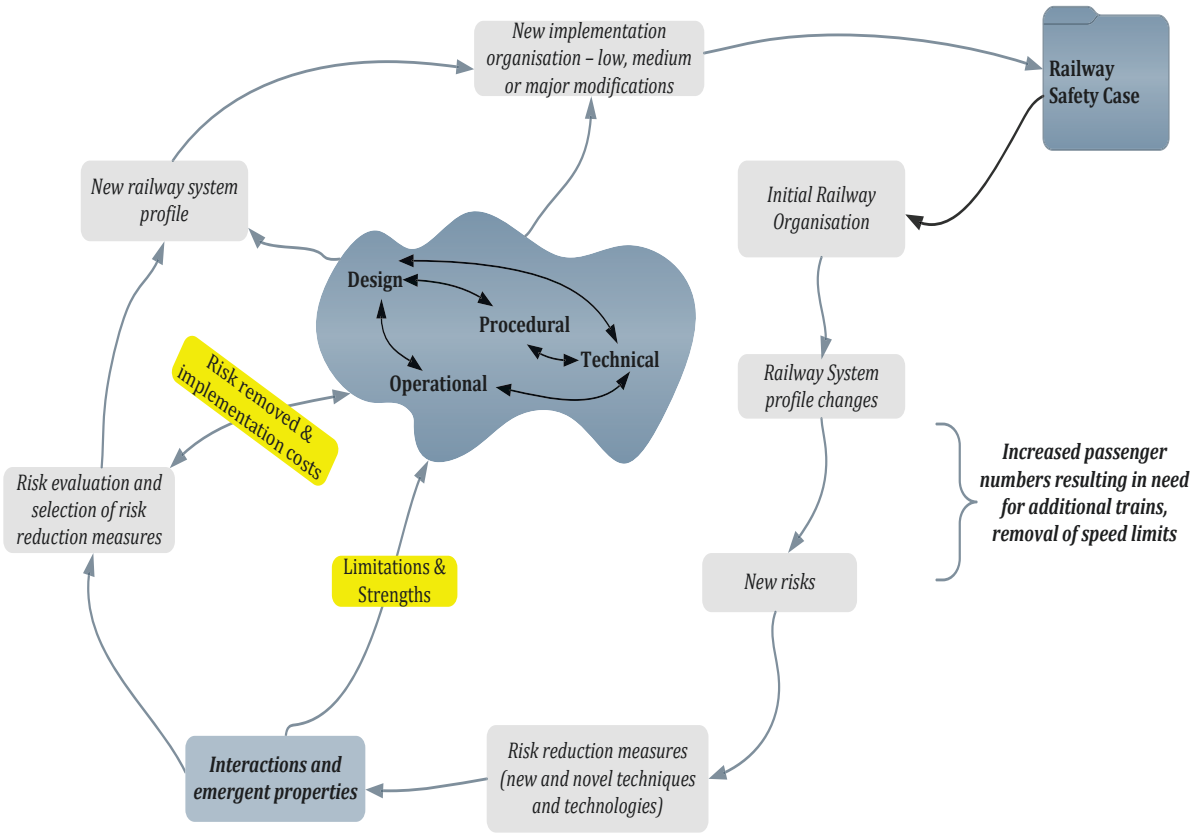


Figure 6: New operational modifications and the process of risk reduction associated with the new risks.

By adopting the proposed categorisation technique, the organisation is less likely to invest in new organisational development and re-structuring schemes that facilitate the required modifications. The assurance of organisational readiness prior to gaining approvals to operate is significantly strengthened by the comprehensive decision-support framework provided by the proposed categorisation. Essentially, it is recommended that to achieve a maximum risk reduction within financial constraints, the concept of *"Readiness for effective risk reduction"* be stipulated as a fundamental process requirement in railway safety cases.

It is essential, that modifications and potential changes to the operating parameters leading to modifications are properly assessed and do not necessarily impose fundamental changes to an existing railway organisation. Without the structure proposed, any rapid evolution of the railway organisation will absolutely result in excessive implementation costs. By improving an organisation's readiness to implement effective risk reduction, significant costs and improved safety levels can be secured.

The DOPT methodology requires a thorough understanding of the budget allocation methodology. This means that as a minimum, the capability of the measure of reducing the likelihood of the accident or the consequences following an accident to be thoroughly understood. The DOPT methodology provides the

framework for reducing the duplication of effort as it supports further considerations of whether the organisation or specific departments within the organisation are better placed to implement the risk reduction measure or combination of measures for any particular risk. The DOPT concept creates also a common risk-reduction platform between departments to ensure synergy in the risk-reduction effort. It supports technical co-operation for the effective use of preventive and protective risk reduction measures to effectively achieve minimisation of railway safety risks. It facilitates establishing and implementing robust accident prevention programmes and mitigation against consequences of an accident.

Conclusions

1. The paper introduced the DOPT classification, derived from basic principles of risk reduction and systems engineering, to address the existing gap between the initiation (evaluation) phase of risk reduction options and the implementation phase. The DOPT methodology creates a common categorisation of risk reduction measures that best addresses a standard railway industry portfolio.

2. The DOPT concept permits effective planning of human resources, spheres of responsibilities and equipment engaged in the risk reduction effort, considering the capabilities of the railway organisation. The clear outline of the roles and responsibilities within the risk reduction context ensures that resources such as finances, technical expertise, information, systems and equipment, medical facilities etc., necessary for implementing the measures are available and appropriately targeted.

3. The DOPT concept promotes a comprehensive understanding of the risks resulting in an accident. It provides a strong support to the Lessons learned database and the check lists related to known accident scenarios.

4. The DOPT concept eliminates the duplication of effort and creates a common risk-reduction platform between departments to ensure synergy in the risk-reduction effort and cooperation at all levels.

5. The DOPT concept is a framework necessary to provide a Level-4 framework that supports risk evaluation, optimal options selection and ultimately permits organisations to maximise risk reduction within a fixed budget. The use of a methodology similar to the proposed DOPT methodology is a characteristic of an organisation possessing a superior level of risk-reduction readiness.

6. In order to achieve a maximum risk reduction within financial constraints, the concept of *"Readiness for effective risk reduction"* must be stipulated as a fundamental process requirement in railway safety cases. The integration of the proposed rational classification structure provides a robust and verifiable case for effective risk reduction.

REFERENCES

1. Van Der Merwe, A.P. (2002). Project Management and business development: integrating strategy, structure processes and projects. International Journal of Project Management 20, pp. 401-411. Elsevier Science Ltd.
2. Van Der Merwe, A.P. (2002). Multi-project management -- organizational structure and control. International Journal of Project Management Vol. 15, No. 4, pp. 223-233.
3. Hobbs, B.; Andersen, B. (2001) .Different alliance relationships for project design and execution. International Journal of Project Management 19, pp. 465-469. Elsevier Science Ltd.
4. Neil, M., Fenton, N. (2005). Tailor M. Using Bayesian networks to model expected and unexpected operational losses. Risk Analysis, 25, pp. 963–72.
5. Williams, T.; Eden, C.; Ackermann, F.; Tait, A.; (1995). The effects of design changes and delays on project costs. Journal of the Operational Research Society, pp. 809–18.
6. Millera, R., Lessard, D. (2001). Understanding and managing risks in large engineering projects. International Journal of Project Management 19, pp. 437–443. Elsevier Science Ltd.
7. Love, P.E.D.; Lopez, R.; GOH, Y.M.; TAM, C.M. (2011). What goes up shouldn't come down: Learning from construction and engineering failures. The 12th East Asia-Pacific Conference on Structural Engineering and Construction. Procedia Engineering 14, pp. 844-850. Elsevier Ltd.
8. Holzmann, V.; Spiegler, I. (2011). Developing risk breakdown structure for information technology organizations International Journal of Project Management 29, pp. 537–546.
9. Gokpinar, B.; Hopp, W.J.; Iravani, S.M.R (2010). The Impact of Misalignment of Organisational Structure and Product Architecture on Quality in Complex Product Development. Management Science Vol. 56, No. 3 pp. 468-484.
10. Hansen, M. T. (2002). Knowledge networks: Explaining effective knowledge sharing in multi-unit companies. Organ. Sci. 13(3), pp. 232 – 248.
11. Carlile, P. R. (2002). A pragmatic view of knowledge and boundaries: Boundary objects in new product development. Organ. Sci. 13(4), pp. 442 – 455.
12. Contractor, N. S.; Monge, P. R. (2002). Managing knowledge net- works. Management Comm. Quart. 16(2) 249–258.
13. Nonaka, I.; Takeuchi, H. (1995). The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation. Oxford University Press, New York.
14. Fang, C.; Marle, F.; Zio, E.; Bocquet, J. (2012). Network theory-based analysis of risk interactions in large engineering projects. Reliability Engineering and System Safety 106, pp. 1–10
15. Corbett, L.M.; Brockelsby, J.; Campbell-Hunt, C. (2002). Tackling industrial complexity. Cambridge: Institute for Manufacturing.

16. Schlindwein, S.L.; Ison, R. (2004). Human knowing and perceived complexity: implications for systems practice. Emergence: Complexity and Organization 6, pp. 27–32.
17. Baccarini, D. (1996). The concept of project complexity - a review. International Journal of Project Management 14, pp. 201–4.
18. Vidal, L.A.; Marle, F.; Bocquet, J.C. (2011). Using a Delphi process and the analytic hierarchy process (AHP) to evaluate the complexity of projects. Expert Systems with Applications, 38 (5), pp. 388 –405.
19. Wong, V.; Shaw, V.; Sher, P. J. H. (1998). Effective Organization and Management of Technology Assimilation - The Case of Taiwanese Information Technology Firms. *Industrial Marketing Management* 27, pp. 213–227. Elsevier Science Inc.
20. Ahonena, J.J.; Savolainena, P. (2010). Software engineering projects may fail before they are started: Post-mortem analysis of five cancelled projects. The Journal of Systems and Software 83, pp. 2175–2187. Elsevier Inc.
21. McFarlan, F.W. (1992). 'Multinational CIO challenges for the 199Os', in Palvia, S., Palvia, P. and Zigli, R.M. eds., The Global Issues of Information Technology Management, Idea Group Publishing, Harrisburg, PA.
22. Zaltman, G.; Dunca, R.; Holbeck, .J. (1973). Innovations and Organizations. Wiley, New York, 1973.
23. Baker, N.R.; Sweeney, D.J. (1978). Toward a conceptual framework of the process of organized innovation technological within the firm. Research Policy 7, pp. 150-174.
24. Remenyi, D.; Heafield, A. (1996). Business process re-engineering: some aspects of how to evaluate and manage the risk exposure. International Journal of Project Management Vol. 14, No. 6, pp. 349-357. Elsevier Science Ltd.
25. Willcocks, .L.; Margetts, H. (1991). Informatization in UK public services from implementation through strategy, to management. EPGA Conference – Informatization in Public Administration, The Hague, Netherlands.
26. Bessant, J. (1991). Managing Advanced Manufacturing Technology: The Challenge of the Fifth Wave, NCC- Blackwell, Manchester.
27. Patanakul, P.; Milosevic, D. (2009). The effectiveness in managing a group of multiple projects: Factors of influence and measurement criteria. International Journal of Project Management 27, pp. 216–233, Elsevier Ltd.
28. Seider, R. (2006). Optimizing project portfolios. Research Technology Management 2006, pp. 49:43.
29. Hendriks, M.; Voeten, B.; Kroep, L. (1999). Human resource allocation in a multi-project R&D environment: resource capacity allocation and project portfolio planning in practice. International Journal Project Manage, 17, pp. 181–8.
30. Nobeoka, K.; Cusumano, M.A. (1995). Multi-project strategy, design transfer, and project

performance: a survey of automobile development projects in the US and Japan. IEEE Trans Eng Manage (42), pp. 397–409.

31. Taleb, N.N. (2007). The black swan, the impact of the highly improbable, Penguin books.
32. Whitty, S.J.; Maylor, H., (2009). And then came complex project management. International Journal of Project Management 27, pp. 304–310.
33. Koppenjana, J.; Veenemanb, W.; Van der Voortb, H.; ten Heuvelhofb, E.; Leijten, M. (2011). Competing management approaches in large engineering projects: The Dutch RandstadRail project. International Journal of Project Management 29, pp. 740–750. Elsevier Ltd.
34. Todinov M.T.; Weli E. (2013). Optimal risk reduction in the railway industry by using dynamic programming. International Conference on Reliability, Safety and Security Engineering, London, UK. World Academy of Science Engineering and Technology.
35. Holzmann, V.; Spiegler, I. (2011). Developing risk breakdown structure for information technology organizations; International Journal of Project Management 29, pp. 537–546.
36. Marshal, C. (2001). Measuring and Managing Operational Risk in Financial Institutions. John Wiley & Sons. pp. 3 – 44. ISBN 978-0471845959.
37. Bessis, J. (2002). Risk Management in Banking. John Wiley & Sons; 2nd Edition, pp. 51 – 67. ISBN 978-0471499770.
38. Railways and Other Guided Transport Systems (Safety) Regulations (ROGS). http://www.rail-reg.gov.uk/server/show/nav.1511. Accessed 29-10-13.
39. Weli, E.; Todinov, M.T. (2013). A new approach to risk reduction in the railway industry. Institution of Engineering and Technology Special Interest Publication - Infrastructure Risk & Resilience: Transportation. pp. 42 – 52. ISSN 2041-5923.