

A PhD RESEARCH PROJECT ON SAFETY RISK ASSESSMENT OF
COMPLEX CHANGES TO RAILWAY INFRASTRUCTURE AND VEHICLES

By

Neil James Barnatt

A thesis submitted to the University of Birmingham for the degree of
Doctor of Philosophy

School of Electronic, Electrical and Systems Engineering
College of Engineering and Physical Sciences
University of Birmingham
July 2021

UNIVERSITY OF
BIRMINGHAM

University of Birmingham Research Archive

e-theses repository

This unpublished thesis/dissertation is copyright of the author and/or third parties. The intellectual property rights of the author or third parties in respect of this work are as defined by The Copyright Designs and Patents Act 1988 or as modified by any successor legislation.

Any use made of information contained in this thesis/dissertation must be in accordance with that legislation and must be properly acknowledged. Further distribution or reproduction in any format is prohibited without the permission of the copyright holder.

Abstract

This study investigates the risk assessment of railway changes in an interconnected environment. Systems are a collection of subsystems and parts, and this thesis develops a new method, the Combined Assessment Method (CAM), to analyse them. CAM potentially applies to many industries, including aviation, defence and nuclear, where there is a requirement to assess system safety objectively. The railway is a specific case of a closely coupled socio-technical system of critical physical interfaces between systems and a stringent example of systems in other industries.

The Author has carried out: an assessment of current techniques, a review of relevant literature, a survey of risk assessment practitioners, an appraisal of current methods, and a review of accident data to identify current accident characteristics.

CAM incorporates established assessment techniques to perform subsystem analysis. Subsystem results are combined using systems engineering methods in a novel way producing an overall risk assessment for a system, which incorporates emergent behaviours.

The assurance of CAM is through a case study and two test cases. It uses safety performance, ease of use, and economic saving criteria to judge success.

Illustrative studies include a metro system, indicating that CAM is potentially a process and is application-independent. Furthermore, test cases illustrate that CAM combines the risks from multiple parts of a whole system into overall risks.

Finally, test cases measure the verification through a match between the findings of official incident reports and the CAM output.

This thesis is the first step to creating CAM as a fully-fledged system safety risk analysis method. Further work is proposed to take CAM forward and address identified weaknesses. Finally, suggestions have been made for further work to “productionize” CAM to increase the likelihood that practitioners in the field will use CAM.

Acknowledgements

I want to take this opportunity to thank my academic supervisors sincerely. First, to Professor Felix Schmid for persuading me to undertake the PhD in the first place and sage comments later on. Second, Professor Anson Jack for his endless patience over the years, incisive comments and steadfast support. Finally, Professor Clive Roberts for picking up the challenge after Anson retired and ensuring that I crossed the finishing line.

Contents

1	Introduction	1
1.1	Previous and interim work	2
1.2	Reasons and context.....	2
1.3	Significance of research	6
1.4	Research questions.....	7
1.5	Limitations	8
1.6	Themes to research	8
1.7	Structure of the thesis	8
1.8	Rationale for the definition of technique, process, and method	13
1.9	Rationale for the differentiation of complex and complicate	14
1.10	Research methodology	14
1.10.1	Potential new method success criteria	19
1.11	Summary.....	23
1.12	Principal points.....	23
2	Literature review	25
2.1	Review of current safety methods	26
2.2	Weighing the outcomes.....	34
2.3	Risk, people and opportunity	39
2.4	Modelling.....	45
2.5	Systems approach.....	46
2.6	Assessment of risk	48
2.7	Possible ways forward.....	51
2.8	Summary.....	53
2.8.1	Principal points	56
3	Industry Information gathering research methods development	58
3.1	Identifying the current methods	59
3.2	Establish technique use	65
3.3	Appraisal of existing techniques.....	66
3.4	Review trends	67
3.5	Information gathering phase satisfaction of research questions.....	67

3.5.1	Technique use	68
3.5.2	Appraise existing techniques	69
3.5.3	Review of trends	69
3.6	Summary	70
3.7	Principal points	70
4	Current methods appraisal, survey and results.....	72
4.1	Survey	72
4.1.1	Development.....	72
4.1.2	Conduct and interpretation	74
4.1.3	Results.....	77
4.1.4	Finding conclusions	94
4.2	Current methods appraisal	95
4.2.1	Assessment conclusions	109
4.3	Summary.....	109
4.4	Principal points.....	110
5	Review of incident data	111
5.1	Incident data.....	111
5.1.1	Method.....	112
5.1.2	Assessment conclusions	115
5.2	Summary.....	117
5.3	Principal points.....	118
6	Composite Assessment Method (CAM) – new model and method	119
6.1	Rationale	119
6.2	Candidates for CAM.....	123
6.3	Method	124
6.3.1	Success for CAM	124
6.3.2	Concept for CAM	125
6.3.3	Architecture of CAM.....	127
6.3.4	Process description of CAM	129
6.3.5	CAM Heuristic for enumerated ‘amplification’ or ‘resistance’	143
6.3.6	Quality control and troubleshooting a CAM analysis.....	144
6.3.7	Developed CAM process	145
6.3.8	Method of choice for the subsystem analysis	146

6.4	Adaption of CAM for post-accident analysis.....	148
6.4.1	CAM Post accident Forward Analysis – (FA).....	148
6.4.2	CAM Post accident Reverse Analysis – (RA)	150
6.5	The three configurations of CAM.....	153
6.6	Simple demonstration.....	155
6.6.1	Risk acceptance	155
6.6.2	Stage 1	157
6.6.3	Stage 2 – subsystem analysis	159
6.6.4	Stage 3 – integrate the analysis.....	163
6.6.5	Stage 4 - rationalisation	163
6.6.6	Stage 5 – summarise the output.....	164
6.7	Summary.....	168
6.8	Principal points.....	169
7	Baildon Rail based comparative analysis case study	170
7.1	Assessment of risk	170
7.2	Use of RAIB reports in the analysis.....	171
7.3	Baildon desktop test case application	173
7.3.1	Test case success criteria	174
7.3.2	Method used	175
7.3.3	Information from the RAIB report	176
7.3.4	List of failures identified from RAIB report	176
7.3.5	Analysis	178
7.3.6	Findings from study and lessons learned	196
7.3.7	Research success criteria satisfaction.....	203
7.4	Comparison of CAM with other methods.....	207
7.4.1	Commentary and discussion	209
7.5	Summary and conclusions	221
8	Rail based application test cases and benchmarking of CAM	224
8.1	Assessment of risk	226
8.2	Grayrigg test case	226
8.2.1	Test case success criteria	227
8.2.2	Brief accident summary from the RAIB report	228
8.2.3	Analysis	229

8.2.4	Findings from study and lessons learned	240
8.2.5	Research success criteria satisfaction	242
8.3	CAM benchmark using the Grayrigg results	246
8.3.1	Summary	252
8.4	Hong Kong metro incident CAM application test case.....	252
8.4.1	Test case success criteria	253
8.4.2	Method used	254
8.4.3	Brief accident summary	256
8.4.4	Source of information.....	256
8.4.5	Analysis	257
8.4.6	Findings from application and lessons learned	271
8.4.7	Research success criteria satisfaction	272
8.5	Summary and conclusions	276
9	Conclusions and further work	278
9.1	High-level conclusive statement.....	278
9.2	Review of the essential points and findings.....	280
9.3	Satisfaction of research questions	283
9.4	Weaknesses and shortcomings	286
9.5	Further work	289
9.6	CAM assessment	291
9.7	Final conclusions.....	294

Illustrations

Figure 1 Chapters and appendices relationship	12
Figure 2 Conceptualised research methodology flow chart.....	18
Figure 3 Risk and understanding matrix, adapted from Boston Consulting matrix reformulated from (Bowman, 1990).....	48
Figure 4 initial survey sectors (Barnatt, 2019a)	73
Figure 5 surveyed sector distribution.....	78
Figure 6 survey sector response	79
Figure 7 Potential competent method use -processed question 3 data.....	81
Figure 8 Potential Method use by infrastructure and other segments	84
Figure 9 Method use comparison.....	85
Figure 10 Percentage of respondent allocating a method to an assessment stage	87
Figure 11 method assignment to process stage.....	89
Figure 12 Assessment approach concerning integration.....	92
Figure 13 Bar table of attitudes to risk acceptance.....	93
Figure 14 RAIB incident reports -raw category totals	116
Figure 15 RAIB reports - incident source analysis.....	116
Figure 16 RAIB reports – the type of incident analysis.....	117
Figure 17 Simple conceptual diagram of CAM	126
Figure 18 CAM system conceptual overview.....	127
Figure 19 Detailed conceptual diagram of method CAM-C	129
Figure 20 Accident diagram in the style of (Rasmussen, 1997)	131
Figure 21 CAM-ERD	131
Figure 22 An example extracted from a CAM-C.....	134
Figure 23 Multi-subsystem CAM-C tracing illustration example	136
Figure 24 CAM-C example extract	140
Figure 25 CAM process.....	146
Figure 26 CAM adapted for post-accident analysis in the forward direction.....	149
Figure 27 CAM adopted for accident analysis in the reverse direction.....	152
Figure 28 Combined CAM method flow diagram.....	154
Figure 29 CAM-ERD Relationship diagram	157
Figure 30 CAM_FN process reproduced from Chapter 6	175
Figure 31 CAM-ERD relationship diagram from Appendix G	180
Figure 32 Analysis processes alignment with facts	214
Figure 33 Risk assessments data usage.....	220
Figure 34 Conceptual depiction of data space	221
Figure 35 CAM_FN process reproduced from Chapter 6	230
Figure 36 CAM-ERD diagram from Appendix E	232
Figure 37 CAM_RA process reproduced from Chapter 6.....	255
Figure 38 CAM-ERD overview relationship diagram from Appendix F	258

Figure 39 Developed CAM-ERD focused on the controller	263
Figure 40 Site layout. Bottom of hill is Trent Way (David Wilson Homes, 2020)	331
Figure 41 Sales vision of path (David Wilson Homes, 2020).....	332
Figure 42 Embankment diagram and water flow from RAIB report	336
Figure 43 Water catchment area for RAIB report	337
Figure 44 Cross-section of culvert from RAIB report.....	338
Figure 45 CAM_FN process reproduced from Appendix J	345
Figure 46 CAM-ERD Relationship diagram.....	348
Figure 47 CAM_RA process reproduced from Appendix J.....	372
Figure 48 CAM-ERD overview relationship diagram	374
Figure 49 Developed CAM-ERD	381
Figure 50 CAM_FN process reproduced from Appendix J	399
Figure 51 Baildon CAM-ERD.....	402
Figure 52 STPA outputs of analysis (Leveson and Thomas, 2018b).....	427
Figure 53 Initial control structure	430
Figure 54 Developed control structure	433
Figure 55 Developed control structure with actuators and sensors overlaid	448
Figure 56 The three variants of CAM	507
Figure 57 CAM_FN variant process	511
Figure 58 CAM-ERD example.....	513
Figure 59 An illustrative example extracted from a CAM-C.....	519
Figure 60 Illustrative CAM-C example.....	522
Figure 61 Multi-subsystem CAM-C tracing illustration example	523
Figure 62 CAM-C example extract.....	526
Figure 63 CAM adapted for post-accident analysis in the forward direction.....	531
Figure 64 CAM adopted for accident analysis in the reverse direction.....	534

Tables

Table 1 Interpretation of (Benner, 1985) criterion.....	20
Table 2 Potential new method success criteria	21
Table 3 Level category of criterion achievement	22
Table 4 List of risk analysis methods reviewed	27
Table 5 List of techniques extracted from the NR SMS (Network Rail, 2018)	60
Table 6 Network Rail SMS risk techniques categorisation	63
Table 7 Risk assessment stage definition	75
Table 8 Risk assessment stage assignment	76
Table 9 Potential competent method use	82
Table 10 Percentage of respondents assigning the technique to the assigned risk assessment stage	90
Table 11 Definition of classifications	96
Table 12 Definition of attributes (reformulated from sources cited in Chapter 2)..	97
Table 13 Risk analysis methods - attributes and qualities.....	100
Table 14 Risk assessment methods - qualities	102
Table 15 Classification definition	112
Table 16 Heading definition.....	113
Table 17 Sample RAIB GB heavy rail accident report extracts reformulated RAIB data	114
Table 18 CAM-C values	138
Table 19 Cause-consequence table extract example.....	142
Table 20 Example risk matrix extract	143
Table 21 Ease of use recommendation.....	147
Table 22 Shorthand name definition.....	153
Table 23 Risk matrix formulated from (CENELEC, 2017)	156
Table 24 Scaling table for occurrence formulated from (CENELEC, 2017)	159
Table 25 Scaling table for the severity formulated from (CENELEC, 2017)	159
Table 26 FMEA for Hill shortcut (shortcut and environment).....	160
Table 27 FMEA for Bike	161
Table 28 FMEA for Rider process	161
Table 29 CAM-C.....	163
Table 30 Rationalised table	164
Table 31 Combined FMEA	165
Table 32 System cause-consequence table.....	166
Table 33 Analysis summary risk matrix	168
Table 34 Calibrated risk matrix based on (CENELEC, 2017)	171
Table 35 Success measure interpretation	174
Table 36 Extracted list of causal factors from RAIB report	177
Table 37 List of failure findings from RAIB report related to the washout event .	178
Table 38 Extract of FMEA for ground integrity (culvert and environment)	183

Table 39 Baildon CAM-C.....	186
Table 40 Example trace	188
Table 41 Extract of the system-level FMEA table.....	194
Table 42 Extract of the Cause-consequence table.....	195
Table 43 Comparison of findings.....	197
Table 44 Baildon risk matrix extracted from Appendix G.....	201
Table 45 Hazards from CAM analysis	202
Table 46 Baildon rationalised risk matrix.....	203
Table 47 Test case success measure	204
Table 48 Risk analysis technique vignettes.....	208
Table 49 Analysis index for methods.....	209
Table 50 Initial hazard identification stage hazard types	210
Table 51 post analysis significant hazards identified.....	211
Table 52 Post analysis cause types	212
Table 53 Analysis density ratios	215
Table 54 Comparison of analysis findings against the official report (Rail Accident Investigation Branch, 2017).....	218
Table 55 Estimated elapsed analysis time and page count.....	219
Table 56 Incident selection criteria	225
Table 57 Success measure interpretation	228
Table 58 CAM-C reproduced from Appendix E	236
Table 59 Grayrigg risk matrix reproduced from Appendix E	240
Table 60 Comparison of findings.....	240
Table 61 CAM application success measure.....	243
Table 62 CAM systems thinking assessment adapted from (Underwood and Waterson, 2013b).....	247
Table 63 CAM usage characteristics assessment adapted from (Underwood and Waterson, 2013b).....	249
Table 64 Success measure interpretation	254
Table 65 Extract of system level cause-consequence table.....	260
Table 66 Reproduced CAM-C system level hazards – consequences.....	262
Table 67 Extract from Appendix F Reformed cause-consequence table indicating the effect of amplification.....	265
Table 68 CAM-C for Zone controller - system level hazards	267
Table 69 Mitigations identified in Appendix F	268
Table 70 Pre-mitigation risk matrix	269
Table 71 Post-mitigation risk matrix	270
Table 72 CAM application success measure.....	273
Table 73 Comparison of selected risk assessment methods	292
Table 74 RAIB GB heavy rail accident report extracts analysis reformulated RAIB data	318
Table 75 Extracted list of causal factors from RAIB report	334
Table 76 List of failure findings from RAIB report related to the washout event .	335

Table 77 Risk matrix formulated from (CENELEC, 2017)	343
Table 78 Systems table	347
Table 79 Scaling table for occurrence formulated from (CENELEC, 2017)	349
Table 80 Scaling table for the severity formulated from (CENELEC, 2017)	350
Table 81 FMEA for switch	350
Table 82 FMEA for train	352
Table 83 FMEA for train people.....	353
Table 84 FMEA infrastructure maintenance people	354
Table 85 FMEA processes	354
Table 86 Grayrigg CAM Combinator	357
Table 87 System level FMEA table	360
Table 88 Cause-consequence table.....	362
Table 89 Grayrigg risk matrix	365
Table 90 Risk matrix formulated from (CENELEC, 2017)	369
Table 91 System level cause-consequence table	376
Table 92 CAM-C system level hazards – consequences	380
Table 93 Reformed cause-consequence table	382
Table 94 CAM-C for Zone controller - system level hazards	386
Table 95 Cause-consequence mitigation table.....	388
Table 96 Pre-mitigation risk matrix	394
Table 97 Post-mitigation risk matrix	395
Table 98 Risk matrix formulated from (CENELEC, 2017)	398
Table 99 Systems table.....	400
Table 100 Scaling table for occurrence formulated from (CENELEC, 2017)	404
Table 101 Scaling table for the severity formulated from (CENELEC, 2017)	405
Table 102 FMEA for ground integrity (culvert and environment)	405
Table 103 FMEA for track integrity	407
Table 104 FMEA for trains.....	409
Table 105 FMEA for people process	410
Table 106 Baildon CAM-C.....	414
Table 107 System-level FMEA table	416
Table 108 Cause-consequence table.....	419
Table 109 Baildon risk matrix	422
Table 110 Baildon rationalised risk matrix.....	423
Table 111 Signaller unsafe control actions.....	434
Table 112 Signalling manager unsafe control actions	435
Table 113 Mobile Operations Manager unsafe control actions.....	435
Table 114 Track Technician unsafe control actions	435
Table 115 Track Section Manager unsafe control actions.....	436
Table 116 Area Controller unsafe control actions.....	437
Table 117 Corporate Operations unsafe control actions	437
Table 118 Corporate Engineering unsafe control actions.....	438
Table 119 Driver unsafe control actions	438

Table 120 Controller constraints to prevent unsafe control actions	439
Table 121 Scenario analysis for unsafe controller actions	449
Table 122 Scenario analysis of controller actions	478
Table 123 Scenario analysis for the controlled process	483
Table 124 Risk matrix formulated from (CENELEC, 2017)	488
Table 125 Interface list	490
Table 126 FMEA for rail system	491
Table 127 Definition of risk components (Rail Safety and Standards Board, 2007)	494
Table 128 Hazard ranking matrix	494
Table 129 Scaling table for severity and occurrence formulated from (CENELEC, 2017)	499
Table 130 FMECA for rail system.....	499
Table 131 Baildon risk matrix	503
Table 132 List of CAM variants	505
Table 133 Stage-page number index	506
Table 134 Risk matrix (CENELEC, 2017)	508
Table 135 Ease of use recommendation	514
Table 136 Modified FMEA column description (Anleitner, 2010) and EN60812 (CENELEC, 2006)	515
Table 137 FMEA sample extract	516
Table 138 CAM-C values	520
Table 139 Cause-consequence table extract example.....	529
Table 140 An Interpretation of the Cause-consequence table columns	529
Table 141 Analysis summary risk matrix	530
Table 142 Reproduced illustrative CAM-C system level hazards – consequences	536
Table 143 CAM-C for Zone controller - system level hazards	537

Appendices

Appendix A	Industry risk analysis survey invitation and questions	307
Appendix B	RAIB GB heavy rail accident report extracts analysis	317
Appendix C	Rationalisation path example particulars	

		329
Appendix D	Baildon incident particulars	
		333
Appendix E	Test case - Grayrigg CAM risk analysis	
		341
Appendix F	Test case - Hong Kong Metro incident CAM analysis	
		366
Appendix G	Baildon incident CAM risk analysis	
		396
Appendix H	Baildon incident STAMP STPA risk analysis	
		424
Appendix I	Baildon incident Yellow Book risk analysis	
		486
Appendix J	CAM user instructions	
		504
References		296

Terms, Abbreviations and Acronyms

Abbreviations and acronyms

Abbreviation or acronym	Description
ALCRM	All Level Crossing Risk Model
ALARP	As Low As Reasonably Practicable
BREXIT	Britain Exiting from the European Union
CAM	Composite Assessment Method
CAM-C	CAM Combinator
CAM-ERD	CAM entity-relationship diagram
CBA	Cost Benefit Analysis
CSM-REA	Common Safety Method for risk evaluation and assessment
DMM	Domain Mapping Matrix
DSM	Domain Structure Matrix
ETA	Event Tree Analysis
ERTMS	European Rail Traffic Management System
FMEA	Fail Modes and Effects Analysis
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
GAO	General Audit Office
GB	Great Britain
HAZOP	Hazard and Operability Study
HF	Human Factors
HSAW	Health and Safety at Work Act
IET	Institution of Engineering Technology
INCOSE	International Council on Systems Engineering
IP	Internet Protocol
IRSE	Institution of Railway Signalling Engineers
MCAS	Manoeuvring Characteristics Augmentation System
NP-Hard	Non-deterministic Polynomial-time-Hard
NR	Network Rail
ORR	Office of Rail and Road
RPN	Risk Priority Number
RSSB	Rail Safety and Standards Board
SCM	Swiss Cheese Model
SFAIRP	So Far As Is Reasonably Practicable
SMOW	Safe Method of Work
SMS	Safety Management System
SORA	Signal Overrun Risk Assessment
SRM	Safety Risk Model
STAMP	System Theoretic Accident Model and Processes
STPA	System Theoretic Process Analysis
SWIFT	Structured What If Technique
THERP	Technique for Human Error Rate Prediction
UK	United Kingdom
YB	Yellow Book

Terms

There are many terms in use within the field of study covered by this thesis; some have varied interpretations. For clarity, the terms listed in the table below have the meaning defined when used in this thesis unless explicitly stated otherwise.

Term	Definition
Accident	A hazard that has been realised, and a loss has resulted.
Complexity	The overall operation has an element of uncertainty and emergent behaviour due to the interaction with its parts.
Complicated	The internal interactions may be intricate and difficult to understand, but nevertheless predictable and repeatable.
Incident	A hazard that has been realised which has resulted in a near miss where an accident has been averted or post event actions/mitigations have dissipated the consequence.
Hazard	An unsafe state of a system that could lead to an incident or accident.
Method	A set of instructions to be followed leading to an outcome, where each step is defined. (The rationale for the definition is given in Chapter 1.)
Process	A set of operations or actions carried out to lead to an outcome. These may be documented in written form or a custom or practice. (The rationale for the definition is given in Chapter 1.)
Root cause	This is the base cause of a hazard within a system.
Summarised risk cause	summarised lower-level hazards which are treated as causes of higher-level hazards/risks, explained in Chapter 6.
Technique	A blend of instructions, implicit knowledge and explicit knowledge applied by using judgement and skill to lead to an informed outcome. (The rationale for the definition is given in Chapter 1.)
Traditional method	This refers to the normal method of risk assessment completing a safety cycle. This involves identifying the hazards and causes afresh (possibly using historical information as a prompt), providing an analysis of the likelihood and consequence, followed by possible mitigation.
Risk	A combination of the severity of a consequence and how often it may occur. (The use of likelihood/ probability and alternative measures for how often a risk occurs is discussed further in Chapter 2.6)

1 Introduction

This thesis has been created out of a long-term interest in railway systems safety engineering, the moral and legal duty driven by society to reduce risk and provide safe systems of transport. Furthermore, at its discretion, a business may wish to reduce risk to a level below the legal limits to match the appetite of the company driven by commercial factors such as a need to be seen to be safer than the competition or reduce liabilities. The requirement to assess risk is applicable to many industries including aviation, defence and nuclear.

This thesis researches the methods of assessing risk. Also, it attempts to indicate whether a new risk assessment process is independent of the railway environment.

The Author has some forty years of experience in the field of railway engineering. Over that period, systems have become more complex as technology has increased. Furthermore, there has been an ever-present pressure to reduce cost, which has resulted in the elimination or reduction of some traditional roles, such as small signal-box signallers controlling a very small section of railway. There has been an increasing focus on improved economic performance with the privatisation of the railway, which has had the effect of separating the train operators from the infrastructure operators.

We live in a very different world from the nationalised railway of those 40 years ago. At the same time, it does not appear that the fundamental approach to safety has radically changed, if at all, from the days when for example the internet as we

now know it simply did not exist and engineering drawings were held on paper. Engineers and operators are expected to carry out risk assessments in this modern world, in addition to the specialist practitioners, resulting in a wide variability of skill level applied to the analyses. Fundamentally, the Author questions if we should still be assessing systems in a similar way to forty years ago? An initial PhD proposal (Barnatt, 2016) was submitted, and this document is a report of the result of the research undertaken.

1.1 Previous and interim work

A co-authored published paper entitled 'Safety Analysis in a Modern Railway Setting' (Barnatt and Jack, 2018) draws on some of the research contained in this thesis to present the objectives of this research and indicate possible ways forward.

1.2 Reasons and context

Taking account of accident reports from RAIB such as (Rail Accident Investigation Branch, 2018a)

Clause 104: 'no risk assessment was prepared for the temporary spur wiring'.

Clause 129: 'Had a risk assessment of the spur wires been carried out, the risk of changes to the interlocking after completion of the test desk design should have been identified and mitigated'.

and (Rail Accident Investigation Branch, 2018b)

Clause 205: 'The risk profiling was based on RSSB's safety risk model²⁰ which is used to understand the overall risk level and risk profile of the main line railway. The safety risk model lists 131 hazardous events. It does not identify a train overturning as a specific event but RSSB stated that the hazard 'derailment of a passenger train' includes the *precursor* 'overspeeding' and that a train overturning is included among the consequences'

Clause 211: 'Had the various risk assessments carried out between 2008 and 2015 recognised the level of risk associated with a tram overturning, it is likely

that the need for additional mitigations, such as improved signage, would have been identified and found to be reasonably practicable to implement'

Recommendation 10: 'This review shall consider:

- i. the extent to which the process for risk assessments is capable of identifying and correctly assessing all significant risks, particularly those related to low frequency/high consequence events; and
- ii. the means by which potential mitigations are identified and evaluated'

Accordingly, it is observed by the Author, that the assessment of risk for large or complex projects or any project involving modern technology is weak in three respects:

First, the approach to railway design is changing from single system changes to a system of systems philosophy, with large scale interaction between the participating systems, which creates new behaviours, as is the case with the Digital Railway¹ changes. This philosophy is best described by the International Council on Systems Engineering Handbook (2015) and the standard EN15288 (2015). Under this regime, many aspects of the railway are changing at the same time creating a complex interaction with the various systems, people and processes. In addition, a change to a single system can have an impact on many other systems, even those that were not directly modified. The original processes such as Hazard and Operability Studies (HAZOP)s, and those captured in DEF STAN 56 (2007) and EN50129 (2003), summarised for the railway in the now withdrawn Yellow Book, (Rail Safety and Standards Board, 2007), did not envisage such an environment because technology at the turn of the century tended to use isolated systems or with limited connection. Interconnection was mostly slow, bespoke and purpose-designed; unlike today with pervasive Internet

¹ Digital Railway is a largescale programme undertaken on behalf of the railway industry with funding managed by Network Rail. Its aim is to digitally enable the railway by connecting systems and using information to create capacity for trains and value for customers

Protocol (IP) high-speed connectivity. The sequential approach encompassed in these systems has been identified by Leveson (2011) as inadequate.

Secondly, current large-scale programmes are not able to scientifically forecast the change in safety risk and therefore weigh capability benefits against risk, other than by using past performance as a guide to future performance through deductive reasoning. A typical technique employed is the Safety Risk Model (SRM), (Rail Safety and Standards Board, 2014b) which uses a set of models based on a collection of 131 low consequence high probability events, such as trips and falls, and high consequence very small probability events monitored over a five-year rolling window. This type of problem has been exemplified by several large-scale changes to the railway infrastructure recently such as Thameslink, and Great Western Mainline programmes, where many interacting features have been changed. In the case of Thameslink, a new signalling system was installed, new trains procured, stations altered, the timetable altered to increase the number of trains, and the trains are to be provided with automatic train control. In the case of the Great Western Mainline new electrification has been installed, major junctions such as Reading have been fundamentally changed, and it introduced a new service. At the time of the introduction of European Rail Traffic Management System (ERTMS) into GB, the radio-based signalling was not present in the SRM. Therefore, the analysis carried out at the time had to approximate the risks using conventional signalling data.

Finally, the legal framework is changing, necessitating more transparent and extensive demonstrations of risk levels, the limits of acceptable risk are changing, and there are potentially conflicting requirements between new and older

legislation. Consequently, there is the potential for a greater level of effort required to create acceptable risk assessments, revised risk limits to be reworked into assessments and extended periods of debate when the results do not satisfy all the requirements. The drive for clearer and more extensive demonstrations is exemplified in the Common Safety Method for Risk Evaluation and Assessment² (CSM-REA, 2013), with the requirement to record and assess all hazards, where this was not previously the case. New limits on quantitative risk have been imposed, through an amendment (CSM-REA Amended, 2015).

There is a conflict between European³ derived law such as the Common Safety Method for Risk Evaluation and Assessment, cited above, and the extensive health and safety law such as the Electricity at Work Regulations (EWR, 1989) where there is a mixture of absolute and practicable duties imposed. In contrast, in the Common Safety Method for Risk Evaluation and Assessment, it is possible to work to prescribed standards to satisfy legal requirements. There is also other European derived legislation that adds to the mix. These combinations are then interpreted in various ways by different parties leading to confusion; which has led to debates between the regulator and Network Rail on electrical clearance distance adequacy for overhead line electrification as an example.

As part Digital Railway project's move to digitally connected railway, the IRSE president set out a view of the requirements from the railway industry to meet the digital railway objective in the IRSE president's speech, Simmons (2015). It proposed a data-enabled railway based on a System of Systems approach where

² This is to be translated into UK law when the UK exits the EU. Therefore, the requirements will remain.

³ Even though the UK has left the European Union much of the legislative requirements have been incorporated into domestic law through a raft of BREXIT legislation enacted 1st January 2021.

the overall rail system is considered holistically using systems theory. During the same year, it appeared to the Author from an IET conference on Safety and Security (2015) in Bristol on 21 October 2015, that the focus of developments and interest was not on safety analysis method development. Rather the focus was elsewhere on cybersecurity. Several of the presented papers referred to expert judgement (McGee and Knight, 2015), (Jarzębowicz and Wardziński, 2015); these focused on single systems; there was a particular focus on merging of safety and security into a single issue (Lobo, Charchalakis and Stipidis, 2015) for example. The nearest paper to align with Simmons (2015) and recognising the issues referred to in this thesis was the paper Sieker (2015) referring to the need to rewrite parts of safety analysis standard EN61508 to tighten the testing claims and thereby increase confidence in the systems.

Research has been undertaken at the University of Huddersfield (Van Gulijk, et al., 2015) to apply methods of collecting 'big data' and using this to mine information for the prediction of railway change project risk. This approach relies on the assumption that past performance is a predictor of future performance.

1.3 Significance of research

This research has sought to refocus risk analysis away from paradigms of single system/change analysis and provide an understanding of safety analysis in a modern railway setting of a system of systems and large-scale changes. Salient gaps in understanding will be identified and addressed where necessary to improve the industry's approach to better weigh the safety risks and benefits within the railway environment.

This research has been conducted and documented in a manner to be generally applicable to the railway industry including when making large scale, complicated or complex changes. Consequently, there is value to the railway industry by providing a basis for judging the acceptability of railway changes, avoiding post-installation rework, before spending large sums of money on the engineering. The approach is likely to be applicable to other complex environments where there are multiple systems such as air transport and the defence sector. The Ministry of Defence has set up a centralised Defence Safety Body, which recognises in a future world there will be much greater interaction between the various systems and branches of the armed forces. The Defence Safety Body could adopt the research contained in this thesis as a standard risk analysis tool.

1.4 Research questions

The refined principal research question is:

Can an understandable new method be developed to analyse and provide an overall risk estimation of system safety risk for railway systems comprised of one or more parts/subsystems that practitioners could use in the field?

These subsidiary questions support the principal question:

1. How should safety hazards be combined in a safety analysis (i.e., where there is an interaction between the parts) to provide a credible overall risk picture without the requirement for expert knowledge?
2. Can a new method be created to identify safety hazards that other methods detect understandably?

1.5 Limitations

The research is focused on the application of risk assessment methods and the critical requirements for a risk assessment method. Issues concerned with the requirements for the approach to the development of risk assessment methods are not addressed.

1.6 Themes to research

The key themes of this research are summarised into four points:

Connectivity – This is a core concern that systems are now interconnected, and changes in one system could affect others. The interconnectivity can lead to the total system having emergent properties and emergent hazards as a result of the connections.

Computerisation – Most physical systems are controlled in some way by products with embedded computers that in turn, affect the physical interfaces, for example, switch control gear that drives the switches.

Usability – It appears that modern methods of analysis are complicated in their own right, and it is questionable in some cases how usable they are by the practitioners in the field.

Overall risk – Often when analysing individual system's, it is not clear what the overall risk effect is on the total system and whether this is positive or negative.

1.7 Structure of the thesis

The structure of the thesis is as follows:

Chapter 2: is a literature review of the previous work in this area and draws out salient knowledge to point to possible ways forward. Papers have been selected

that review the legal basis for risk assessment, the critiques of current methods, a review of the limitations of human understanding. Part of the review covers papers that propose new and adapted techniques. Relevant points are summarised at the end of the chapter for further consideration in the research later in the thesis.

Chapter 3: sets out the research methodology in terms of a survey to be undertaken and an appraisal of existing techniques. The appraisal provides a vehicle to convey an understanding of the techniques currently in place in the hazard analysis process. The chapter develops a rationale for the methods used in the subsequent chapters and how they provide the material for a new method.

Chapter 4: provides an assessment of the current assessment methods in two parts: first, an industry survey and an analysis of the data to identify key findings. Second, a desktop appraisal by the Author of features and attributes of each current method, to highlight the strengths and weakness. The analysis will draw on the material developed in Chapter 2 to define attribute categories.

Chapter 5: presents an assessment by the Author against criteria of incident data. The aim is to identify trends to consider when creating a new method. The review is focused on differentiating between a single system and multi-system incidents. Accordingly, this provides evidence of whether treating systems as isolated entities when undertaking a risk assessment reflects how accidents occur.

Chapter 6: describes a new method of hazard analysis created by the Author. It utilises data gathered from chapters 2, 4 and 5 together with insights to provide a framework. Assurance is provided by testing the new method as described in chapters 7 and 8. Feedback from tests is incorporated as part of the method

development, which leads to the finalised method presented at the end of the chapter.

Chapter 7: consists of a selected rail-based case study to compare the performance of three methods of risk assessment to benchmark the proposed new method. The chapter shows that the proposed technique identifies the key hazards identified by others with salient additions. It shows that relatively the technique is quick to use and therefore is more economical. Furthermore, it demonstrates that the proposed technique identifies, physical, people-based and whole system hazards without the bias indicated by the other techniques.

Chapter 8: describes two rail-based illustrative application test cases that are selected to test and highlight features of the new method. One of the test cases is used as a benchmark study using a test case that has been reported for other techniques; in this case, Lambrigg (Underwood and Waterson, 2013b). The chapter shows that this proposed technique identifies the hazards that are identified by an official report together with additions. The proposed technique is applied in two modes to different problems that indicate the method's flexibility and is economical to apply.

Chapter 9 draws together the insights and results to draw conclusions and make proposals for further work. The chapter reflects on the research that has been undertaken summarising the key points. It justifies the satisfaction of each research question. A consideration of the limitations of the research is presented together with areas for further development of the research.

Figure 1 shows the relationship between the chapters and the supporting appendices. A short rationale for the appendices is attached where the need is unclear.

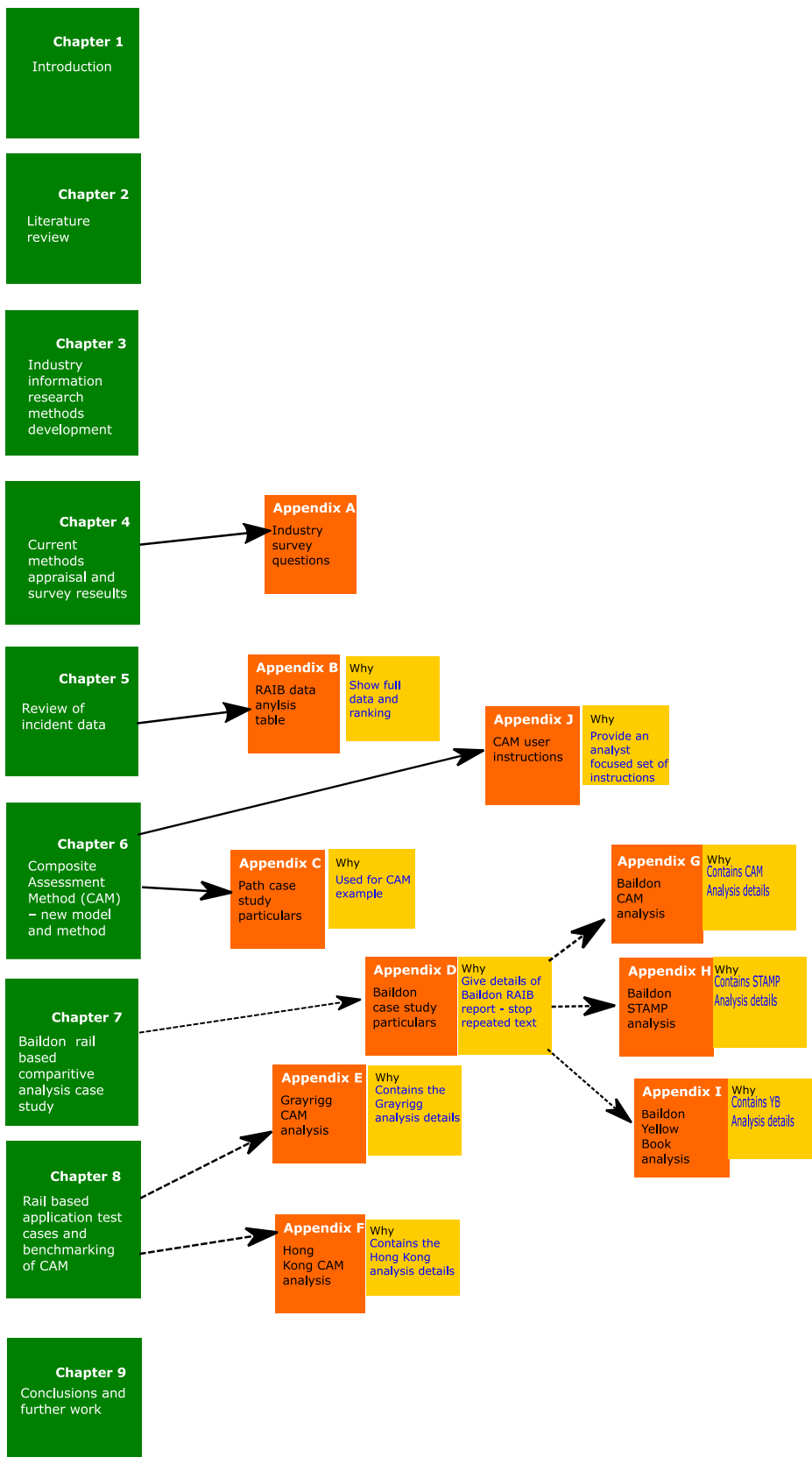


Figure 1 Chapters and appendices relationship

1.8 Rationale for the definition of technique, process, and method

The terms defined in this section are in common usage with multiple meanings.

Therefore, they are defined for the purposes of this thesis.

A **method** is defined as ‘a special form of procedure’ by (*The Concise Oxford Dictionary of Current English*, 1979), and a procedure is defined in the same publication as ‘mode of conducting business or legal action’. A slightly different perspective is offered from a systems engineering standpoint with a **method** defined as ‘used as a given, much like following a recipe in a recipe book’ by (The Open University, No Date). In this case, the essence of the meaning is taken to be a set of instructions or steps.

A **technique** is defined as ‘mode of artistic execution in music etc; mechanical skill in art; means of achieving one’s purpose’ as defined in the same publication by (*The Concise Oxford Dictionary of Current English*, 1979). While (The Open University, No Date) defines a **technique** as ‘Technique is concerned with both the skill and ability of doing or achieving something and the manner of its execution’. In this case a composite meaning is taken that this refers to undertaking a task, part using skill.

A **process** is defined as ‘series of operations in manufacture, printing, photography etc’ by (*The Concise Oxford Dictionary of Current English*, 1979). In this case the meaning is clear.

This thesis uses the meaning of these definitions described in the Terms section at the beginning of the thesis.

1.9 Rationale for the differentiation of complex and complicate

The words complex, complexity and complicate, complicated appear frequently in this thesis, however, from the dictionary definitions they appear very similar in meaning. **Complicate** is defined as 'Mix up make complex or intricate' while **complex** is defined as 'Consisting of parts, composite; complicated' by (*The Concise Oxford Dictionary of Current English*, 1979).

INCOSE (2015) when defining a system of systems refers to the two terms being different claiming complicated is where there are interactions between many parts being 'governed by fixed relationships.' While complex systems are stated to have parts which 'exhibit self-organization' and 'local interactions give rise to emergent patterns.' It also implies that complication is not a prerequisite for complexity.

Sargut and McGrath (2011) also refer to the difference between complicated and complexity. Stating that complicated things for the most part obey rules and their outputs are predictable and repeatable, whereas in complex systems the patterns are changing creating uncertainty and emergent behaviour as a result. The uncertainty they attribute to the interconnectedness among other things. This view is supported by Kamensky (2011).

In this thesis complicated is taken to mean that the interactions may be intricate and difficult to understand, but nevertheless predictable and repeatable.

Complexity is taken to mean that the overall operation has an element of uncertainty and emergent behaviour due to the interaction with its parts.

1.10 Research methodology

Figure 2 shows an overview of the research methodology. It is divided into three main sections: information gathering, development and assurance. The first task is

to gather evidence from various sources and weigh this to decide if a new system safety risk assessment method is justified. If a new method is warranted, proceed and develop a new method and test it using case studies as examples. The results from the tests are fed back to refine the method and address shortcomings. The tests also provide assurance that the new method is fit for purpose by successfully applying it to several scenarios. Sections of the methodology are developed further in Chapter 3, where there is a focus on obtaining information from the industry. Results from this process will form the material for the thesis conclusions. The success of any proposed new method will be judged separately using success criteria.

Originally it was envisaged that a workshop would form part of the assurance evidence. However, it became impractical to implement with the advent of the Covid-19 epidemic and the associated social distancing. Instead, the other strands of the assurance were enlarged.

Case studies have been chosen as the assurance method because it is a technique that is widely used in research as cited by Rahim and Baksh (2003) and Teegavarapu and Summers (2008). They are defined by Teegavarapu and Summers (2008) as an

‘empirical research method used to investigate a contemporary phenomenon, focusing on the dynamics of the case, within its real life context’.

In this particular case, they are used as a review mechanism set in a pseudo-real-life situation. Furthermore, the American audit office (GAO) (United States General Accounting Office, 1990) defines a case study as:

‘A case study is a method for learning about a complex instance, based on a comprehensive understanding of that instance obtained by extensive description and analysis of that instance taken as a whole and in its context.’

It reinforces the concept of instances taken and analysed, which aligns accident/incident reports used in this thesis. The GAO cites different types of case studies, in particular, those that study an instance of the application of a method or policy in a particular setting are labelled as ‘illustrative application case studies’. It states that these are characterised as ‘descriptive’ and in-depth.

The weakness in accident case studies is that the information available is limited by that released by the official investigation bodies. The GAO report, (United States General Accounting Office, 1990), indicates that a qualifying quality of a case study is that it is an in-depth study. Comparing the output of an analysis to a single official report could be argued to disqualify the case. A full case study is undertaken to address this weakness, which compares the output against the official report, with further comparison drawn with the output of other representative risk analysis methods. The combination provides several different points of reference, which adds to the depth of the study.

The other 'case studies' carried out in this thesis are rebranded as 'application test cases', which represent 'mini-case studies' where limited points of comparison are provided.

A collection of a case study and application test cases are used to avoid bias and indicate wide applicability which will improve the external validity of the research. Furthermore, this approach provides evidence based on actual real situations rather than contrived circumstances, increasing the confidence, where a case study or test case is successful, that it will work in the field. If a case study or test case fails, this would call into question the validity of the new method unless the failure can be explained as being attributable to other factors. Each case is judged in isolation against a set of predefined criteria, and supports the demonstration of internal consistency. This method of testing is a form of negative logic that serves to give assurance that the process is not skewed towards producing positive answers.

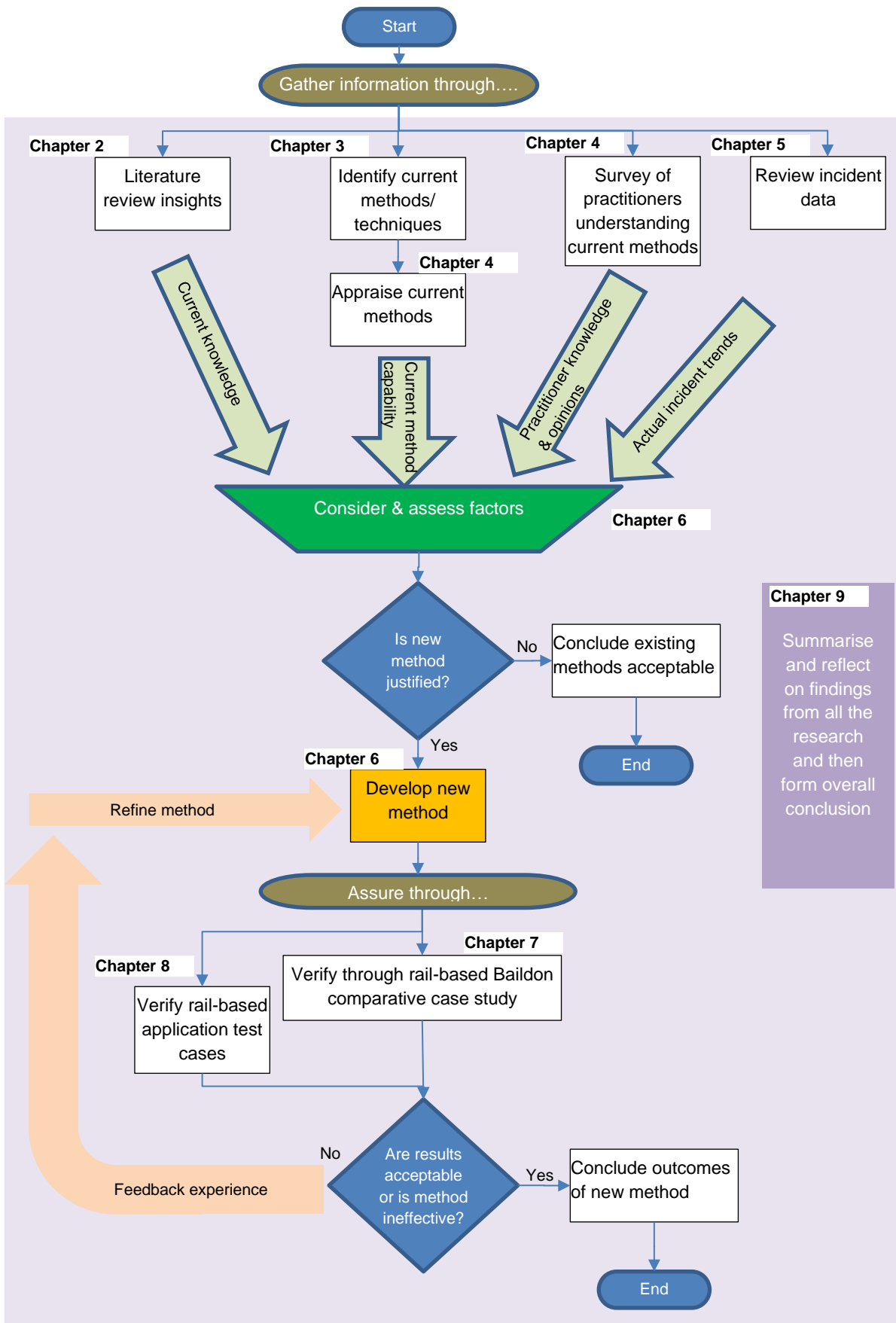


Figure 2 Conceptualised research methodology flow chart

1.10.1 Potential new method success criteria

New methods are weighed against success criteria developed by the Author to gauge whether it is acceptable. There is a limited set of assurance data emanating from the case study and test cases. Consequently, it is not viable to ascribe quantitative measures of success. Instead, qualitative measures have been selected, as is advised by Rahim and Baksh (2003). The criteria developed have been influenced by the studies of Benner (1985) who analysed and ranked safety methods and investigation methodologies. These criteria were partially set to indicate the compliance to legislation and the organisational remit of the safety authority. Criteria such as non-causal refer to the influence of other models on the model under consideration, rather than in the sense of a causal model. A full description of each is given in (Benner, 1985). His studies identified ten critical types of criteria each for safety models and methodologies under various captions. These are summarised and interpreted by the Author under four headings as safety identification, efficiency, applicability and transparency. The ten model criteria classifications are shown in Table 1.

Table 1 Interpretation of (Benner, 1985) criterion

Criterion	Headings			
	Identification	Efficiency	Applicability	Transparency
Realistic	✓	✓		
Satisfying			✓	
Comprehensive	✓			
Disciplining		✓		
Consistent	✓		✓	
Direct	✓	✓		
Functional		✓	✓	
Non causal				✓
Visible				✓

The efficiency category refers to minimisation of effort, which is categorised for the research as an economic classification. The transparency category, although important, is subjective and does not lend itself to a small time-limited dataset. The first three have been interpreted in Table 2 below:

Table 2 Potential new method success criteria

Category	Criteria	Measure
Safety	In a comparison setting: As a minimum, the same hazards are identified as other methods. In a required finding setting: Other specific safety criteria met.	Case study/application results where a comparison with previous studies can be made. Or where other safety criteria are set these should be met when the method is tested without comparison.
Economic	An efficient method of performing the analysis.	Case study/application results demonstrating that analysis is possible without resort to computing and teams of analysts. This can be expressed as understandability. In practical terms it is measured as the relative effort in time and volume of output or meet predefined limits.
Applicability	Applicable to railway engineering safety risk assessment problems with single and multiple systems. Ideally, to also be applicable in other fields.	Case study/application results demonstrating applicability where multiple systems are present. In addition, a demonstration of applicability to another field.

The economic criterion is the most difficult of the three criteria to objectively demonstrate in a case study environment because it is not an observable field attribute. In essence, the criterion is a measure of the ratio of effort and reward. Benner (1985) refers to the rapidity of creating new knowledge as an economic measure through event-based analysis during his analysis of 10 years of safety data, which is a subjective measure. In terms of case studies, an objective measure could be the number of cycles through the process. However, the complexity of the subject of the case study will heavily influence the process cycles. Where a time and volume target are set these objective measures should be met; although they will only provide a relative measure of effort and reward

against the beliefs of an arbitrary benchmark or norm because they influenced by complexity. Accordingly, the Author has additionally selected understandability as a more robust surrogate measure for the economic category, which is not subject to the same confounding variable of the measurement of cycles.

Understandability, is an essential element of competent analysis, as described in Chapter 2.

The success criteria have been defined on a generic basis. Each of the criteria will require refinement and possible reinterpretation to meet individual test case criteria, for example in cases where there are no results from other methods for comparison. However, the objective will be to create a logically equivalent set of criteria.

A simple linear scale has been chosen to rate the case studies against the criteria, which is similar in concept to Benner (1985). The spectrum runs from failure to success, where success is deemed as all criteria are met while failure is all criteria are missed, with other values depicting partial success. A higher level of success is judged to be achieved when expectations are surpassed. The levels are tabulated as follows:

Table 3 Level category of criterion achievement

Level	Description
Surpassed expectations	The measure was met in full and exceeded by achieving a higher level than required. This is classed as a success of the criterion.
Successful	The measure was met in full and is classed as a success of the criterion.
Partial success	The measure was met in part with some deficiencies. This is classed as a qualified success of the criterion.
Failure	The measure was not met at all and is classed as a failure of the criterion.

1.11 Summary

This chapter has described how the research contained in this thesis could lead to an improved safety risk assessment process for the railway. A research question and supporting subsidiary questions have been created to judge the success of the research.

The roles of the chapters and appendices have been described and shown in Figure 1. A strategy for carrying out the research has been created and shown in Figure 2, it has divided the research into three phases gathering information, creating a new method and providing assurance that the new method is a valid safety risk analysis method.

A falsification approach has been taken to the assurance validation of a new method, where a failure of a test would show that the method is not valid. An assurance method using test cases has been put forward together with a set of success criteria involving three categories that provide a balanced view of success.

1.12 Principal points

The following are the principal points from this chapter:

- i. The reasons for undertaking the research have been described with the objective of improving the safety risk analysis within the railway environment
- ii. The research question and two subsidiary questions have been formulated and provide a reference to test the success of the research

- iii. The structure of the thesis has been laid out and divided into data gathering, new method creation and assurance
- iv. The research method using test cases has been justified
- v. Success criteria have been created for the test cases covering safety, economic and applicability categories

2 Literature review

The purpose of the literature review is to establish the present state of the art in the field of system safety and identify gaps in current knowledge. Accordingly, it will provide a reference to show that the outcomes of the research are new. There is a great deal of material on the engineering of railways. However, it has become clear that there are few specific railway safety method publications; this may be due to system safety being a generally applicable engineering concept. However, by including material from associated fields, reasonable coverage has been obtained.

The review has been conducted by obtaining papers and documents mainly from online searches. The primary source was the University of Birmingham library catalogue via the library 'find-it' search engine. Additional searches were conducted online using the 'google scholar' search engine. The Author used past extensive experience in the field to select search criteria, which were names of known authors and methods in the subject area together with keywords from within the domain, such as 'acceptance', 'risk', 'ALARP', 'complexity', and 'consequence'. Papers were also obtained from INCOSE, IRSE periodicals, RSSB website, the government legislation website, and the government treasury website. The bibliography from reviewed papers was used to identify further salient papers to expand the coverage of the subject matter. This material was then filtered by the Author to provide a salient review. An indication of the number of papers reviewed can be obtained from the bibliography.

2.1 Review of current safety methods

There are in effect three distinct themes to risk analysis methods, Technical, Human Factors and Organisational, with the latest theme created as a combined analysis of the other themes, termed Sociotechnical, as cited by Leveson (2011), Aven (2008) and Hollnagel (2012) among others. The sociotechnical analysis is heavily weighted towards human and organisational effects. The approach deviates from the traditional approach by looking for deviations rather than errors, that said, deviations are still analogous to errors of some description. Some of the traditional techniques date back to the 1950s, although in that respect, there is nothing wrong with age if the fundamentals are valid. These traditional techniques focus on the technical aspects of risk analysis.

The Author has chosen to categorise the techniques as 'traditional', 'sociotechnical' and 'others' for reference in later chapters. Traditional techniques are defined as technical focused; they have been used for decades.

Sociotechnical techniques are defined as those that focus on managerial and organisational aspects of risk. The others category captures those that do not fit into the traditional and sociotechnical categories, new technically focused techniques for example.

Representative risk analysis methods selected for review in this chapter are shown in Table 4.

Table 4 List of risk analysis methods reviewed

Method	Theme			Category			Reference
	Technical	Human factors	Organisational	Traditional	Sociotechnical	Other	
Accimap		✓	✓		✓		(Svedung and Rasmussen, 2002)
Bayesian Networks	✓					✓	(Marsh and Bearfield, 2008)
Formal Method 'B'	✓					✓	(Boulanger, 2014)
Failure Modes and Effects Analysis	✓			✓			(Anleitner, 2010)
Fault Trees	✓			✓			(Aven, 2008)
Functional Resonance Analysis Method		✓	✓		✓		(Hollnagel, 2012)
Safety Risk Model	✓					✓	(Rail Safety and Standards Board, 2014b)
Swiss Cheese model		✓	✓		✓		(Reason, 1997) (Reason, 2016)
Systematic Theoretic Accident Model and Process		✓	✓		✓		(Leveson, 2011)

A discussion led by the supporters of sociotechnical analysis methods has centred on the continued validity of the traditional techniques and approach; it is outlined in the following paragraphs.

Leveson (2011) has asserted that current methods have an implicit assumption that controls have a sequential relationship and that this is not how modern equipment operates. Furthermore, Leveson (2011) asserts that these methods do not analyse the analysis subject as a whole system; Section 2.5 addresses this aspect. The Swiss Cheese Model (SCM) was one of those criticised for being sequential. Nevertheless, contrary opinions had previously been expressed by Reason, Hollnagel and Paries (2006) in a EUROCODE report. The report made two important assertions that the SCM is not sequential, and the intent was never to have a detailed model. Further, it states that the suitability of SCM depends on what the model is used for and lists communication device, analysis tool, and measurement system as suitable uses.

Other models were also criticised as not fit for purpose such as the Failure Modes and Effects Analysis (FMEA) method, where again it can quite clearly be seen from Anleitner (2010) for example, that it is also not sequential in concept. Other models, documented by Aven (2008) and Rail Safety and Standards Board (2007), fall into the same camp such as Fault Trees (FTA) and event trees fit into a similar mould but differ in that they create graphical logical relationships between risks, causes and consequences. The Author has concluded that Leveson (2011) is expressing frustration that some of the methods do not appear to cope well with scale, complication and complexity.

FMEA is an example of an adapted method that could be considered cumbersome to scale. Initially, it was developed as a failure identification method as part of a quality toolset to improve product performance. For complete system analysis, many individual FMEAs may have to be performed, one for each main component,

as noted by Anleitner (2010). This exercise may be considered cumbersome. Aven (2008), notes its use in safety analysis as a well-understood technique. Anleitner (2010) highlights that failures are considered individually; consequently, there is no notion of chaining as asserted by Leveson (2011). Lepmets (2017) describes how to convert failure occurrence to a rate consistent with safety events. Mohr (2002) provides an example given to Madison-Wisconsin University IceCube Neutrino Observatory project. Consequently, there is ample evidence that FMEA is still a suitable technique for safety analysis, but may take effort and resource to apply correctly. This analysis supports the Authors assertion that scalability is the underlying issue.

A clear example of a non-sequential system is a modern computer system where the code may have latent errors that only require trigger conditions to be present for the fault to arise, a property that has also been attributed to other environments by Rasmussen (1997). For software-based systems, the HSE, (Bishop, Bloomfield and Froome, 2001) for example, shows the expected level of latent error. It goes on to indicate that errors in code will emerge over time as different functions get exercised, and only as a result of use will errors be discovered and eliminated.

The notion identified by this earlier work can be combined with Leveson's concept of control to map out a technological world where risk cannot be totally controlled. Rasmussen (1997) arrives at similar conclusions and proposes a concept of operating limits that when crossed lead to an unsafe condition. Leveson (2011) goes on to suggest that the only practical way to examine systems is by using systems theory concepts and proposes a generic method called System Theoretic Accident Model and Processes (STAMP). This generic method has been refined into usable methods such as System Theoretic Process Analysis (STPA) as

described in Leveson and Thomas (2018b) and is proposed for use in a railway setting by Dunsford and Chatzimichailidou (2020). However, this model appears to concentrate on the managerial and rule-setting parts of risk rather than the 'sharp-end' as Reason (1997) refers to the operational systems. A further feature of STAMP is an examination of the hierarchical nature of the management control as exemplified by the diagram (Leveson, 2011, p.82). Reason (1997) and (2016) SCM also gives a great deal of weight to the latent errors in the managerial layers rather than operational modelling. The Functional Resonance Analysis Method (FRAM) as proposed by Hollnagel (2012) again concentrates on the managerial aspects and almost treats the technical system as passive. In practice, in the railway, these newer models, FRAM and STAMP will be constrained at the industry level by the fixed organisational requirements of industry-specific legislation such as (ROGS, 2006) and a characteristic of the railway identified by Rail Safety and Standards Board (2014c). Moreover, Dunsford and Chatzimichailidou (2020) assert that STAMP does not meet the requirements of CSM-RA as required by law. It is noted from Leveson and Thomas (2018b) that STAMP'S STPA variant does not explicitly identify causes which is a hindrance in an analysis.

It appears that the traditional models such as FMEA, FTA and event trees have much more focus on the 'sharp end'. It may well be that the 'newer' models are well suited to procedurally controlled environments where there is a very high reliance on human accuracy. However, projects employ engineering solutions, as cited by Institute of Railway Signalling Engineers (2005) for example, to prevent incorrect decisions and guide the humans to the correct action; consequently, the

correct operation of the technical equipment is essential and therefore technical analysis is still essential.

Underwood and Waterson (2013b) have set out to compare the various methods as applied to investigations, taking the example of the Grayrigg rail accident. They conclude that provided the limitation that SCM does not go into the detail is acknowledged, then it is a suitable systems approach, especially as it offers a relatively simple concept. This simplicity is a big plus in a complex environment. The paper supports this view by stating that STAMP, developed by Leveson (2011), is thorough but is complicated without the ability to summarise a system on a page and while suitable for researchers is not really practicable for those in the field. In the paper by Underwood and Waterson (2013b), the method used by the Australian Transport Safety Bureau is tested. It is a development of the original SCM and fills in some gaps by incorporating a layered approach to safety. There is a diagram, (Underwood and Waterson, 2013b), that seems to suggest that the SCM is sequential. It is easy to draw this conclusion from the words of Reason (1997), where there is a clear reference to layers and defence-in-depth, followed by a sequential organisational descriptive model. The model appears to have been influenced by Heinrich's (1920's) dominos, that links organisational factors to workplace factors, which in turn link to unsafe acts. There is clearly a need for some interpretation to conclude that it is a system's, non-sequential theory. A comparison of Reason (1997) and (2016) model architecture with (Leveson, 2011) STAMP model and its STPA derivative (Leveson and Thomas, 2018b), shows that the method's organisational influence analysis suffers from precisely the same issue of a hierarchical, hence sequential, organisational influence.

Reason, Hollnagel and Paries (2006) describe how the Swiss Cheese model was developed. It describes how accidents could be equated to pathogens in a body in that 'latent conditions' exist that can combine with a trigger to cause accidents in the same way as a cake will rise if baked with yeast but yeast on its own is not enough to do anything. This analogy appears to fit well with both errors in engineering standards, procedural type of errors as well as software. For example, errors in procedures will not be activated if the particular action is not called upon, as was the case in the three-mile island accident (Whittingham, 2004).

Leveson (2011) makes several claims for system safety supported by examples:

1. "High reliability is neither sufficient or necessary for safety.
2. Accidents are complex processes involving the entire sociotechnical system. Traditional event chain models cannot describe this process adequately.
3. Risk and safety may best be understood and communicated in ways other than probabilistic risk analysis.
4. Operator error is a product of the environment in which it occurs. To reduce operator error, we must change the environment in which the operator works.
5. Highly reliable software is not necessarily safe. Increasing software reliability will only have minimal impact on safety.
6. Systems will tend to migrate toward states of higher risk. Such migration can be predicted and prevented by the appropriate design or detected during operations using leading indicators of increasing risk.

7. Blame is the enemy of safety. Focus should be on understanding how system behaviour as a whole contributes to loss and not on who or what was to blame for it.”

Claim 1 appears to be intuitively correct with the Mars lander and Herald of Free Enterprise examples used are compelling. This claim could be extended to include cybersecurity. Claim 1 is further enhanced with the assertion that safety is a system property and not restricted to components. Claim 2 is in two parts; the first part does appear to be farfetched when considering accidents in the round. Causes will vary across the board statistically. The second part does have support from others, such as Reason (1997), who proposes a parallel approach. Claim 3 appears to be presumptuous and more of a view than anything else. The first part of claim 5 has support from Bishop, Bloomfield and Froome (2001); however, the assumptions in the second part are not necessarily supported. Claim 6 was originally proposed by Rasmussen (1997), who suggested that operating systems near safety boundaries controlled risks better. It appears that Rasmussen (1997) is taking the opposite view, that risk arises from an unconscious drift to the safety boundaries. Claim 4 has been supported by other writers such as Whittingham (2004) who clearly articulates that deficiencies in system design increase the likelihood of human error. In effect, the maxim is to design machine interfaces to fit humans and not the other way around even though often humans are seen as a cheap point of flexibility in a system. Extending this further leads to a conclusion that there are limits to human understanding which includes processes, mentioned by Whittingham (2004) who among others considers that humans are part of a total system.

2.2 Weighing the outcomes

The need to evaluate comes from legal requirements that are set in statute by the Health and Safety at Work Act (HSAW Act, 1974) which requires risks in many cases⁴ to be reduced So Far As Is Reasonably Practicable (SFAIRP) which is otherwise formulated as As Low As Reasonably Practicable (ALARP) for engineering purposes. It is important to understand that this term originates from case law as a judgement by Lord Asquith in the case of *Edwards v The Coal Board* 1949, as reported in many sources, (SWARB, 2016) for example cite the ratio decendi as:

“Reasonably practicable’ . . . seems to me to imply that a computation must be made by the owner, 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.’ “

This implies that risk is not always eliminated and could materialise; consequently, society should not be outraged and surprised when, on rare occasions, accidents happen. The question should be; were suitable assessments made with what could be reasonably foreseen at the time? Foreseeability is another key concept that is written into law (HSAW Act, 1974), section 6, for example. The judgement gives rise to the need to evaluate safety benefit against cost. The big problem with this judgement has always been ‘grossly disproportional’ was never defined; therefore, there is no absolute ratio that provides a cut-off. There has been a subsequent questioning of the judgement *Jones-Lee, et al.* (2006) because of the

⁴ There are exceptions where different duties are imposed either through regulation via sections 15 and 33 of the Act or in the Act itself; for example, section 5(1) requires the use of ‘best practical means’ to prevent harmful emissions.

age, the uncertainty of 'gross' and what appears to be non-conformance to normal financial justification rules. The concept of disapplication on the grounds of age has recently been effectively challenged in a court case in the Supreme Court over BREXIT; the court has firmly refuted the notation that the age of legislation or judgement is a reason for the disapplication. In this case, (*Miller*, 2017), reference was made to old legislation and cases dating back to the 1600s. All the law was found to be just as relevant today as when it was first muted. Consequently, irrespective of the popularity or otherwise of the Edwards judgement it appears the only way to alter the judgement on reasonable practicability and by inference the uncertainty surrounding the definition of 'gross' is to appeal to the Supreme Court or pass legislation. The court could, for example, redefine the test of reasonable practicability in a new judgement or legislation could be brought to replace the term with something else.

The evaluation of the output to determine balance within the legal framework that mitigation is required is normally done via a cost-benefit analysis, which is a general business analysis tool. The application of this method is described by Ed. Laylard and Glaister (1994) in a social environment such as a transport system with a safety implication. Ed. Laylard and Glaister (1994) make it clear that a whole life view must be taken of a project where costs and risks from future years should be included and related to the present values using Net Present Value. A paper from Jones-Lee, chapter 9, is included that describes a set of six considerations for assessing safety:

- Ignore the cost and make safety number one at any price;

- Use informal methods, otherwise known as gut feel or personal preference;
- Use safety standards or targets; these must be pre-prescribed;
- Cost-effectiveness to measure the benefit within a fixed budget;
- Estimate the benefits using a cost-benefit approach;
- Decision analysis using, for example, Multi-Attribute Utility Theory (MAUT).

Jones-Lee chapter 9 in (Ed. Laylard and Glaister, 1994) makes a case for the use of CBA through several stages. First Jones-Lee disposes of the first two considerations as un-scientific and not practical. Jones-Lee goes on to question the basis of the third, standards, by asking if the basis of the validity of the criteria used to develop the standard in the first place is sound. The line of questioning is based on the notion that a standard is simply a level to be met and therefore, could be wasting money by imposing high-cost solutions. It may not deliver the best safety benefit. This finding has implications for the Common Safety Method code of practice process specified in EU regulations (CSM-REA, 2013), which uses a standards approach. The concern is because the finding implies that the application of a code of practice may not result in the best solution in terms of an acceptable safety benefit at minimum cost.

Jones-Lee takes a similar line in (Ed. Laylard and Glaister, 1994) to the cost-effectiveness approach where there is a distinction drawn between spend and safety benefit. With this method, the emphasis is all on the actual expenditure. The implication is that spend is not necessarily an indicator of a wise spend from a safety perspective. For a railway industry that is resource-limited, again this has

implications. It implies that spending money does not necessarily result in a better outcome.

Jones-Lee, chapter 9, in (Ed. Laylard and Glaister, 1994) dismisses the MAUT approach stating in effect 'that it provides the decision-maker with the tools and framework to come to the preferred outcome'. An alternate view is proposed by French, Bedford and Atherton (2005) from the nuclear industry who propose the MAUT as a viable method of defining an ALARP solution. The paper argues that value is a combination of the science (risks, for example), and values which is a personal preference element. The advantage put forward for this method is each stakeholders' views can be considered, and those views can be weighted depending on the importance of the stakeholder instead of the single view of the CBA approach. In addition, that value has meaning from the individual rather than the CBA collective. For some risks, this has merit, especially where there is a large group of different powerful stakeholders, as is found in the rail industry.

Jones-Lee, in (Ed. Laylard and Glaister, 1994), goes on to discuss the value of human life. There is a discussion of many aspects, including the tax regimes and wealth, but in the end, comes to state that the almost universal approach adopted by governments is a 'gross output' based valuation. The value per life concept has been translated in the UK by the government to a statistical value of a life model as discussed in Jones-Lee, et al. (2006) undertaken on behalf of RSSB, drawing on the official published government risk assessment advice, known as the Green Book (HM Treasury, 2011). This risk value is composed of a gross output element and cost of recovery, as detailed in (Jones-Lee, et al., 2006). In the UK, the government publishes a value which for the rail industry is published by RSSB

(Rail Safety and Standards Board, 2019) at £2.017M, which is not out of line with values from surveys put forward by Jones-Lee that range from £250k to £2M. RSSB produced a guide (2014a) on CBA and how to convert the value of a life into a CBA benefit. It states that this should be done by multiplying the benefit in terms of Fatality Weighted Injuries by the Value of Preventing a Fatality (VPF), in this case, that would be £2.017M as published by RSSB (Rail Safety and Standards Board, 2019).

Jones-Lee, et al. (2006) points out that in reality, the VPF is miss-named and stands for a value that society as a whole is willing to pay to prevent a statistical fatality. It is made clear that it is a small improvement in safety that could result in zero or more preventions of a fatality. Therefore, the concept is merely a reference that moves up and down following a societal framework benchmark. Moreover, it should be treated as such. The fact that it is accepted through the CBA mechanism, Jones-Lee, et al. (2006), as a measure by the courts is what gives it importance and is implicit in the Edwards judgement (SWARB, 2016).

The method is in common use within the rail industry. The guide takes a narrower view of CBA benefits than is implied in Ed. Laylard and Glaister (1994). As cited in Taking Safe Decisions (Rail Safety and Standards Board, 2014c, p.20), which points to (Rail Safety and Standards Board, 2014a) CBA guide which suggests that only the safety benefits should be taken into account and weighed against the capital and maintenance costs. While this simplifies the analysis, it does omit any commercial or societal benefit that may also be gained. Instead, it asserts that commercial decisions are distinct from safety decisions. At the micro-component level, the approach appears to be sensible by increasing the likelihood that the

option offering the greatest economic safety benefit is adopted and meets the letter of UK law.

For programmes such as the electrification schemes (Network Rail, 2016), of which the Great Western Mainline electrification is a part, it raises the issue of how the creation of a new railway subsystem is justified because it introduces an electrocution risk that was not present before. It seems obvious that the social benefits described by Ed. Laylard and Glaister (1994) have to be part of the calculation at the macro level otherwise on strict safety grounds the CBA would always produce a case for sticking with the existing diesel trains. Ed. Laylard and Glaister (1994), state this calculation should be performed by taking the existing benefit and adding an average fare of those willing to pay and then for those to whom the benefit is marginal add half the extra benefit again to obtain the total benefit. By subtracting the risk values, a CBA figure is obtained. Through this process, it is possible to conclude that benefit to society is gained by increasing the safety risks taken. The CBA guide, (Rail Safety and Standards Board, 2014a), in appendix B, suggests that this kind of benefit should be considered for inclusion which appears to step away from the position in the main text. On balance, from this analysis of the reviewed CBA literature, at the macro level, it does appear that societal benefit is a legitimate subject for inclusion.

2.3 Risk, people and opportunity

A theory of homeostasis⁵ has developed around road safety (Wilde, 1998). There has been an adoption of changes to road safety legislation based on this theory.

⁵ Homeostasis is the phenomenon of people taking additional risks to compensate for safety improvements. For example, driving a car more aggressively because it has an antilock brake system than if it had not.

More to the point, a critical mass of support was achieved that made change possible, as cited in Adams (1994), although the participants may not have been that well informed. The acceptance of the theory has not exactly been universal with some stating in strident terms that it is flawed (O'Neill and Williams, 1998). However, even these detractors admit that there is something in it that describes a human predisposition to take advantage of advances. Reason (1997), argues much the same when he refers to safety advances being turned into production advances which tend to cancel the original safety benefit. Rasmussen (1997) asserts that operations drift toward the safety limits as a natural mechanism because there is pressure to operate close to the limit to extract commercial advantage. It appears perhaps that there is a three-part answer: first, there is an imperative to operate at the edge of acceptability to remain competitive. Second, therefore, as additional facilities become available operations and users move to a 'riskier' position because they can and finally, perhaps this is a more realistic explanation of homeostasis. What it does imply is that mistakes can be made, as Rasmussen (1997) notes.

Further, Rasmussen (1997) notes that accidents are often through normal work set in train far in advance, with little inconsequential errors adding up to an unsafe condition with an accident just waiting for a trigger, which is often a human. This idea was later developed into the Accimap method by Svedung and Rasmussen (2002) which specifically looks at the role of small latent errors in accidents.

Dekker (2005, chapter 2), refers to a similar drift, citing Rasmussen and Svedung (2000) in an analysis of what is termed the 'New View' of human factors analysis. The 'New View' philosophy asserts that human error is a symptom of other

problems and that blame appears to be directed toward the hierarchy of the organisation or the physical systems. Furthermore, Dekker (2006) asserts that it is the role of Human Factors specialists to defend individuals, consequently there may be an element of bias. More concerning is Le Coze (2022) paints an unflattering picture of Dekker as someone who has driven the New View but is unjustifiably confrontational with Reason's ideas and an anarchist. In his historical critique, he states that most of Dekker's ideas are Woods ideas that are repackaged and "weaponised". He further refers to the notion of the New View as better referenced as the school of Cognitive System Engineering and Resilience Engineering, which takes in the works of Hollnagel (with FRAM), Woods (2018) (with Graceful Extensibility theory) and Dekker as a collective due to the spread of ideas and philosophy from the authors. There are further concerning essays such as Cooper (2022) in "The Emperor has no clothes: A critique of Safety II" who roundly criticises the New View collective as being without proper foundation and "circular". Moreover, the criticism goes on to deride a characterisation of Dekker's view that human errors do not exist. In effect, Cooper articulates a point-by-point demolition of the New View. Cooper concludes that because of the antagonism it is unlikely that the Old View and New View schools will combine into a unified position. In the light of these comments caution is called for before accepting the ideas of the New View and casting anything off from the Old View championed by Reason. Le Coze (2022) clearly states there is a great deal of merit in Reason's ideas of human error, with slips, trips and mistakes. Equally there is merit in Woods (2018) idea of adaptability and brittleness when adaptability cannot cope. In summary there are effects of human activity, there may be various ideas of how these effects are triggered, but nevertheless it has to be recognised that these

effects sometimes have a detrimental effect on the system which has to be analysed.

Dekker (2005) and (2006) asserts that these errors often appear to be the right thing to do at the time under the prevailing local conditions and primarily it is this that differs from the 'Old View' of human factors. This notion makes detection difficult at a later point in time. Furthermore, Dekker (2006) asserts that these 'errors' are symptomatic of deeper issues with the system as a whole, including at the organisational level which points to the need to understand the whole system. The requirement for a system review is supported by Salmon, Walker and Stanton (2015). However, they take a different approach to the concept of loss of situational awareness which they assert is a systems level attribute and not a component level or an individual attribute. In addition, they assert that there are many contributors to incidents including individuals.

Dekker (2006) articulating the New View, asserts that there is a variance between procedures written at the corporate level and what is actually carried out on the shop floor. This phenomenon is supported by Reason (1997). Furthermore, the local drift is a series of small deltas from the official position to suit local conditions, eventually amounting to a chasm that introduces significant risk. Yet, at the same time, operators and engineers use these local methods to comply with all requirements. Consequently, the drift could be unnoticed.

Considering all these 'New View' ideas does not explain why track workers, for example, are killed on the railway. For example RAIB in their investigation report (Branch, 2017) concluded that distraction played a role, but it could be argued this does not cover all root causes. Overall, there appears to be some substance to

New View, that some “human errors” are caused by systematic or organisational failings, but by no means all. On balance it is clear that Reason’s “Old View”, or “mainstream” view as Cooper (2022) refers to it, should continue to be used, but supplemented at the edges with New View concepts such as an understanding of what operators may have been thinking at the time, brittleness and drift.

Therefore, operating at the limit may be useful but operating beyond it is not, and it is critical to prevent this excursion and detect it. In that light; it appears that there is at the limit a need for robust technical safety controls. Furthermore, it implies that there are many causes for accidents that combine to initiate the event. It also implies that seemingly small risks may at the system level eventually prove disastrous.

There are also limits to human understanding to the extent that Whittingham (2004) cites Rasmussen’s Skills Rules and Knowledge (SRK) model as a way in which humans cope with complexity. Whittingham (2004) notes that most tasks are either delegated to a skill or rule where the sequence is predetermined, and only a single task can be undertaken that requires a new sequence to be deduced because of the cognitive load. Reason (1997) cites this type of approach as humans attempt to simplify problems and points out that errors can be introduced, such as selecting a bad rule, known as ‘mispliance’, which results in an unsafe outcome. The Common Safety Method (CSM-REA Amended, 2015) uses a rules-based approach, called ‘Code of Practice’ as one of the risk evaluation principles if a code exists and is relevant. This approach presupposes that a code of practice remains ‘good’ which may not be the case when technology changes or connections that did not previously exist between systems are put into place.

Users are often not in a position to challenge the codes without the underlying knowledge of how the Code of Practice was created, potentially leaving them exposed. There is a further danger that a Code of Practice is seen as an easy option leading to a checkbox mentality without understanding the true risks which is a factor cited in the Nimrod air disaster report (Haddon-Cave, 2009) as a key failing. Therefore, Codes of Practice should be used with caution.

Modern systems inevitably become more complex, and complicated to understand and analyse as different parts are connected. There are limits to understanding as is exemplified by chess problems with many pieces on the board. The sequence of moves to win is not understood because there are too many variations. Good players and chess masters apply rules of thumb to win based on analysis of previous games, which is an example of an SRK approach. However, when there are few pieces, the game becomes readily analysable by humans. Manson (2001) refers to the problems of complexity for humans influencing a point at which they cannot be understood due to three types of complexity: algorithmic, deterministic and aggregate. Algorithmic complexity is a reference to the difficulty of constructing equations to understand the system. Deterministic complexity is associated with being able to determine an exact answer in an environment where small changes could have a big influence on the output. Aggregate complexity refers to emerging behaviours of systems and the interrelationships of coupling strengths. Chess falls into the algorithmic and deterministic problems while modern connected systems fall into a mix of algorithmic and aggregate areas. To be understood, it would appear that the level of complexity has to be controlled

and systems engineering attempts to control this through encapsulation⁶ and division of the whole into parts. Furthermore, it is likely that where there is complexity the propensity for error is increased, especially where the human is left unassisted by rules and processes. Whittingham (2004) cites THERP and SRK figures which show an order of magnitude improvement in errors where a process is applied for complex tasks. This indicates that defined analysis processes are another mechanism to assist the analyst in controlling complexity.

2.4 Modelling

An alternate approach is to create models of the systems under analysis.

Modelling is currently an expensive exercise that demands resource, data and time. RSSB on behalf of the industry has created a Safety Risk Model (SRM) (Rail Safety and Standards Board, 2014b) that provides a generalised model of risk for the current rail network. This model has been in existence for many years. As currently constructed, the retrospective model has been critiqued by Turner, et al. (2002), it is based on a rolling window⁷ of past performance data and therefore cannot really predict future performance if the network is changed even with the integrated fault and event trees because the whole model is based on the existing status quo. It is, however, a good predictor of risk in the static network, but not good for network reconfiguration or novel installations.

Bayesian networks are an alternative event tree modelling method. Marsh and Bearfield (2008) have proposed using Bayesian networks to model large networks from a safety perspective. This technique is complicated because of the need to

⁶ Encapsulation is taken to mean enclosing an item in a container and exposing only the critical features that interface to the outside world which describe the external effect of the inner workings.

⁷ A rolling window is a span of time, say 3 years for example that moves along the timeline. Say this window was initiated at the year 2000 it would span 2000 to 2002 inclusive. When the year moved to 2001 the window would now span 2001 to 2003 inclusive.

create joint probability distribution tables (JPTs)⁸, as described by Bayesia S.A.S (2020), for each vertex⁹. JPTs are a collection of conditional probability tables (CPTs) for each state of the variables feeding into a vertex. This technique leads to a large-scale matrix puzzle that is beyond human understanding and requires computerisation. For an analyst in the field, it would prove to be a challenge to analyse a practical problem and understand the implications of the result. Even if powerful computers are available to analysts in the field, specialist software would be needed to carry out the complicated matrix computations. It does, however, have the advantage of combining probabilistic causal links with a logical combination element which does not feature in many of the other methods.

2.5 Systems approach

Systems engineering has dealt with complexity through scope by imposing a boundary to limit the extent of a system. This approach has been documented in the Systems Engineering Handbook (INCOSE, 2015) in detail. The framework has been published to a wider audience through the systems engineering lifecycle standard ISO15288 (International Standardization Organization, 2015). It is clear from these publications that as subsystems are connected, behaviours emerge that were not analysable within the subsystem. This notion can be extended to risk analysis, so risks that were not apparent at lower levels which emerge at higher-levels can be identified. The notion is supported by Leveson (2011) and (2016) who asserts that the nature of accidents is changing. Leveson (2011), further asserts that only simple systems are understandable and complex systems can only be understood superficially. It appears that in this conundrum, the details that

⁸ A joint probability distribution table is the probability of all events that could happen due to the inputs to that vertex.

⁹ A vertex is a node (or joining point) in a network linked by arcs to other vertices in the network.

cause the emergent unsafe behaviour, and consequent hazard, could be missed and knowledge of the detail is essential to be able to recognise a potential hazard. Again there are linkages with Rasmussen (1997), as previously discussed, who describes the small errors summing to a hazard that later emerges. The Author deduces from the previous comments that it is critical to accurately select from a myriad of data only those outputs from one subsystem that affect another in a key way to avoid the complexity problem.

Systems transmit or receive effects through either physical means, energy transfer or information transfer. The first two means are visible and measurable while the latter is often unseen except in the effect on the receiving system if it causes an action or reaction to take place. In that respect, causes can pass unnoticed when driven by unseen software. Software is often complex and is sometimes critical to the operation of the overall system; for instance, the Typhoon Eurofighter, (Posey, 2012) would be unstable without software, or the ETCS system. Bishop, Bloomfield and Froome (2001) have indicated that software is in commercial operation with latent errors present, which are reduced through corrections which can introduce yet more errors. It is reasonable from the evidence described to conclude that software will always have a population of errors unless testing can exercise every conceivable combination of input variable. Current methods, as described by EN50128 (CENELEC, 2011), rely on process controls to limit the population rather than specific error elimination. This reliance is because the software is currently not fully analysable. Efforts have been made to eliminate these errors, and by inference, the associated hazards, through formal methods

such as 'B'¹⁰. However, it has been acknowledged that formal methods only prove the requirements development of the Abstract Machine and that it is perfectly possible to produce unsafe output even though the 'B' process states that it is correct, as reported by Boulanger (2014).

It is concluded by the Author from the previous paragraphs, that there are two types of complexity, internal algorithmic and collective aggregate, which is aligned to Manson (2001). The level of complexity will affect the number of unknowns and misunderstood features of a system. In turn, this will affect risk. This understanding-complexity-risk relationship is depicted as an adaption of the Boston Consulting Matrix

		Risk	
		Known	Unknown
Complexity ↓	Understanding	Known	Specification
		Unknown	Design/operation outcomes
		Complexity →	
		General industry knowledge	
		Unknown unknowns	

Figure 3 Risk and understanding matrix, adapted from Boston Consulting matrix reformulated from (Bowman, 1990)

Therefore, to limit risk and complexity, it would appear that understanding should increase and complexity reduced, which is an objective of the systems engineering decomposition into smaller units.

2.6 Assessment of risk

Some of the 'newer' methods (Leveson, 2011), (Hollnagel, 2012) do not directly consider risk in the traditional way. For example, there appears to be an emphasis on performance variation. In this light, it is reasonable to question what risk

¹⁰ B is a formal language used to describe requirements and logical associations.

actually is and the validity of its expression. In practical terms, risk is described as a consequence multiplied by a frequency, and it is traditionally linked to a probability. Edwards (1992) states to be mathematically correct that probability must obey three rules:

- equate to a value of 1 for certainty and 0 for an impossibility,
- use a consistent evaluation model, and
- each instance to represent a unique event.

In a risk identification processes such as HAZOPs (International Electrotechnical Commission, 2001) the objective is to draw in as many items as possible from participants in a workshop. It is used as a mechanism to ensure completeness. Consequently, it is unlikely that the uniqueness requirement is met, it is also unlikely that if all outcomes were considered, the total would sum to 1. Furthermore, the data is influenced by previous experiences and bias of the participants, rather than a demonstrable frequency of occurrence. It is more appropriate to refer to likelihood instead of probability as this meets the rules of likelihood as expressed by Edwards (1992) and Pawitan (2001). It would appear that, if accepted, this undermines Bayesian networks and other probabilistic methods of analysis because likelihood does not obey probabilistic mathematical principles, as shown in detail by Pawitan (2001). Kahneman (2011) models the human mind as two conceptual systems and notes that it is 'inept' when considering probabilities which raise further questions about the reliability of probabilistic assessment. Instead, Kahneman (2011) asserts that humans answer simpler substitute questions using heuristics and associations together with feelings about the subject of the question. However, Shafer (1976) resolves the

problems by asserting that when assessing an unknown where there is a possibility of incomplete information, for example, it is a person's belief in an outcome that is being expressed rather than a strict probabilistic value, Kahneman (2011) use of feelings is similar to belief.

Shafer (1976) is of further help in stating that the judgement can only be assessed on what is known at the time and that the data set is restricted by practicalities.

This assertion is supported by Kahneman (2011) who coins the phrase 'what you see is all there is' when making judgements, which translates into assessments can only be made on what is known. Finally, Shafer (1976) adds the concept of plausibility to be the lack of evidence against an event which produces the highest probability value. This plausibility concept is possibly a better way of considering and evaluating causes in a risk analysis because the most pessimistic view will be considered, which aligns with what the law requires, where the ORR requires consideration of the worst-case credible outcome as cited in the handbook (Office of Rail and Road, 2018). The work by Shafer (1976) building on Dempster's theory is developed to allow the use of probabilistic relationships between elements. This development neatly provides an explanation for the use of likelihood/belief/probabilistic forms and relationships. There has been criticism of Shafer's work by Pearl (1990) among others, that it does not adequately address the areas of incomplete data, extended data and pooling of knowledge. Pearl (1990) points out that in some cases, it produces non-sensical results. These criticisms are levelled from an artificial intelligence learning perspective which appears to be a more generalised field than the constrained problem of risk identification and analysis.

Nevertheless, the belief theory continues to be popular, being widely cited, and in the context of risk assessment overcomes several apparent difficulties. In conclusion, it would appear that the use of quantitative and qualitative values is appropriate even in the absence of comprehensive data. Furthermore, given that in essence beliefs are being used that variances from an arbitrary norm cited in the 'newer' techniques, such as FRAM, is an equally valid method of expressing risk as it too, in essence, is an expression of belief.

2.7 Possible ways forward

Design Structured Matrix methodology, as described by Eppinger and Browning (2012), offers an intuitive method of mapping relationships between entities. It is a development of an established systems engineering interface mapping called N^2 , defined in the handbook (INCOSE, 2015). It is a system engineering technique for understanding how parts of a system interact with each other. There are two fundamental types of map described by Eppinger and Browning (2012), a Design Structured Matrix (DSM) and a Domain Mapping Matrix (DMM) which are combined in various combinations into an overall Multidomain Matrix (MDM). However, the schema has a limitation that a DSM can only map relationships in a single system domain while a DMM can be used to map between domains. In the context of multiple systems, as addressed by this thesis, it is of more significance to consider how to link systems together using a DMM. This schema provides the opportunity to document both static and dynamic information. Bonzo, McLain and Avent (2016) develop the concept slightly by asserting that by squaring a DMM it is a special case of a DSM and a bi-directional relationship can be mapped. The DSM provides the static element for both a product component relationship and organisational teams relationships. DSMs can also be used to depict temporal-

dynamic relationships, as described by Bonzo, McLain and Avent (2016). Eppinger and Browning (2012), highlights throughout that the binary information of a relationship can be augmented with additional meanings. It occurs to the Author that a safety relationship or influence relationship could be simply documented in this way. As an example of the potential Bonzo, McLain and Avent (2016) describes an adapted application for a hospital operating theatre. However, although this is based on system engineering and the efficiency case, it is easy to envisage an adaption for safety information of complex systems. Another feature of this method is that it is not necessary to understand all the details of the components before undertaking an analysis; the only requirement is to understand how the relationship is formed. Eppinger and Browning (2012, p.49-53), provide many examples of a top-down approach, such as the development of a new drone by NASA for Mars contractors.

The DSM approach has been proposed for assessing the viability of new businesses by De Lessio, et al. (2015), who use the approach to create a multi-layered process. This proposal has its attractions because the first layer is used to simplify the problem at hand. Secondly, the paper introduces the concept of change propagation where links between parts of the system are identified as multipliers, carriers and absorbers. Although the paper is approached from the perspective of creating a model of multipliers for financial analysis, the concepts can be extracted and applied to a safety environment.

A similar idea from the perspective of reliability has been proposed by Parmar and Lees (1987). It uses the concept of links between systems to model the propagation of faults. This idea has again taken the concept of links having

properties that can be modelled through equations, although in this case, some of those relationships may well be complex. By using the ideas of De Lessio, et al. (2015) to simplify the equations to multipliers, carriers and absorbers the complication of a model developed along these lines can be contained.

2.8 Summary

The information gleaned from the literature review is used throughout the thesis and forms an essential basis for the development of a new method in Chapter 6.

Section 2.1 has highlighted those new techniques, such as STAMP, tend to focus on the management and organisational risks, rather than those at the operational level. Much of this hierarchical focus is redundant in a railway setting because the framework is predetermined through railway specific legislation as described in Section 2.1 and indicated by Rail Safety and Standards Board (2014c). There is, however, an advance with the newer techniques, through the recognition that in a modern setting, systems are composed of other significant parts beyond just the physical system of interest.

There is a single method of weighing safety benefit and risk, which is set in legislation, as described in Section 2.2. Therefore, it is futile to propose other methods to evaluate benefit because the courts will not accept it unless it is aligned with the legal principles of SFAIRP or the legislation is changed. It is interesting to note that far from a social perception that risks should not be realised; realisation of risk is a distinct possibility and is recognised in law, through the concept of reasonableness.

There are three identified acceptable ways of evaluating a risk assessment set out in the law, compliance with Codes of Practice or risk estimation combined with

CBA; the third method is simply a comparison with an existing installation showing parity of function and by inference risk as a method acceptance. It has been noted that societal benefits should be taken into account when carrying out a CBA. A Code of Practice, on the other hand, only requires compliance, but these codes have been shown to have an associated risk of 'mispliance' or encouraging tick-box checking. Therefore, if there is doubt in a situation, the risk analysis followed by a CBA will most likely produce the best results.

The criticisms from Leveson (2011) that existing established analysis systems are sequential is not necessarily grounded. The literature review in Section 2.1 has demonstrated that highlighted techniques do not exhibit a sequencing of any kind and shown that the authors have shown the contrary as in Reason, Hollnagel and Paries (2006) for example. The criticism is more likely frustration that some of the techniques do not scale well to new types of system in their current form.

Therefore, far from being obsolete older techniques appear to be equally applicable, although they have a technical rather than human or organisational focus.

In a modern system, information flow is often a key ingredient, as in ERTMS, but modern risk analysis systems do not appear to address this directly. To a lesser extent, the same is concluded for the human interaction role within the systems. It appears from the literature review; the interaction between subsystems during risk analysis is ignored unless an overview analysis is undertaken, which risks missing key details because it takes a high-level view of the total system. This risk has been asserted by Leveson (2011), for example, to be the case with the traditional methods of analysis which do not take a whole system approach. It is evident that

If there is a concentration on the subsystem level, then behaviours of the system may not even be present to evaluate any attendant risk, a property of systems highlighted by INCOSE (2015) and discussed in Section 2.5. Consequently, the Author concludes that both subsystem and system-level analysis is required.

There have been some writers that have identified complexity as a problem. In particular limits on human understanding have been identified which limit the capacity for effective risk analysis. This limitation is likely to be the case for interconnected systems. A remedy appears to be to split systems into understandable elements and selectively recombine the links between them to gain an overview, which follows a system engineering philosophy. It was shown in Section 2.3 that understandability is a critical part of the analysis, and that simplicity helps that process. The section also indicates that the analysis is further improved when it is carried out using a defined process.

Moreover, in Section 2.5, it was shown that decomposition aides understandability. Furthermore, Section 2.7 shows through the work of Eppinger and Browning (2012) that the parts can be brought together to create a whole system view. This potential solution will be tested through the research carried out in this thesis.

There has been a move away from the traditional risk measurement in the newer techniques towards assuming that the normal state is safe and deviations are where risk is present, for example, in FRAM. As described in Section 2.6, the argument over risk measurement in terms of probability has been ongoing. It has been concluded by the Author in alignment with Shafer (1976), that in reality, the method adopted is nothing more than a belief set to some scale and what really

matters is the quantum of belief relative to the other beliefs in a particular area. In effect, a qualitative or quantitative analysis will be equally effective as long as the risks are identified with the correct quantum. Consequently, it is asserted by the Author, after consideration of the literature, that it is equally acceptable to use any method as long as it is consistent for the system under consideration.

There has been a discussion in sections 2.4 and 2.7 of ways to combine subsystem analysis into a full system overview. Bayesian networks have been proposed, but suffer from a high mathematical and computational requirement to process the JPTs for each vertex which leads to complication. It has been concluded from the literature review that DSM and DMM offer a realistic way to selectively recombine small subsystems into a whole. This method potentially provides a way of eliminating non-essential links to increase the level of understandability for the analyst.

From the literature review sections 2.1, 2.5 and 2.7 it is clear that an overarching risk assessment could be carried out, however, as stated it may well suffer from a lack of detail that is buried at the subsystem level, which could lead to missed hazards or complexity putting the analysis beyond understandability. It has been shown in Section 2.3 that simplicity in the analysis is critical for understanding and that analysis at both the subsystem and full system level is essential for hazard coverage. These themes will be tested through the research in this thesis.

2.8.1 Principal points

The following are the principal points from this chapter:

- i. Sociotechnical techniques, such as STAMP and FRAM concentrate on management and organisational risks. These risks are not relevant because the railway is regulated
- ii. Legislation is clear the risk acceptance is required to match SFAIRP
- iii. Codes of Practice should be used with caution in case they become outdated
- iv. Societal benefits should be taken into account when undertaking a CBA
- v. Criticisms of traditional methods for sequencing is not well founded
- vi. Information flow is a key ingredient in modern systems, but modern risks analysis does not account for it
- vii. Subsystem and system-level risk analysis is required to account for risks in a system
- viii. Complexity is an issue for human understanding of the risk assessment process and therefore affects the quality of the analysis

3 Industry Information gathering research methods development

The strategy, outlined in Chapter 1, is to gather information, decide if a new method is warranted, develop a new method, and assure the method. This chapter focuses on developing research methods to obtain additional information from the industry to supplement the literature review and set the findings in the context of railway safety risk assessment as currently practiced.

The railway industry has a series of standards and processes that companies apply to comply with the legal, business and moral requirements for managing risk. The Health and Safety at Work Act (HSAW Act, 1974) encapsulates legal requirements as an obligation to control risks to an acceptable level. The processes and standards in the railway industry specify techniques that are judged suitable to meet the legal requirements. An example is a requirement in legal regulations of HSAW, (ROGS, 2006), is to write and operate a Safety Management System known as an SMS to control how safety is assured. Furthermore, the legislation requires that incidents meeting set criteria are reported to and in some specified cases investigated by the Rail Accident Investigation Branch (RAIB) and that the reports are published. Reports published by RAIB provide evidence to use in the research.

A four-point approach is taken to analyse the railway assessment environment:

- Establish what techniques current practice indicates should be used;
- Establish if the techniques that should be in use, are in use;
- Review the features, strengths and weaknesses of current techniques; and,
- Review the trends from incident data.

A justification of how they address the research question set out in Chapter 1 is given in section 3.5 after the development of the research strategy.

3.1 Identifying the current methods

The railway is operated through a series of companies that receive authorisations and certificates from the safety regulator (in this case the ORR) as their authority to operate. Operators receive these authorisations in response to a submission of a SMS document that sets out, at a high level, how safety is managed, including change management. It is reasonable to expect that operators will abide by the contents of the SMS. Network Rail in a departure from the norm has a particularly detailed SMS (Network Rail, 2018) which identifies several risk assessment and identification techniques and is used as the starting point for the identification of risk assessment techniques.

Some SMS techniques are bespoke tools used within the company to assess specific risks, such as the All Level Crossing Risk Model (ALCRM) or the Signal Overrun Assessment (SORA) Risk Model, they do not address general risks with projects and operation. These tools are designed to provide a specific simplified answer to projects implementing changes to level crossing types or addressing issues with signalling layouts. They avoid the need to undertake a detailed safety risk assessment. Therefore, ALCRM and SORA are not considered further in this research which is concerned with general risk analysis techniques.

Most projects are multidisciplinary and rely on specialist analysts to provide a safety assessment of the acceptability of the project outcomes. Table 5 lists the general techniques available in SMS. A paragraph explains each technique listed in the Network Rail Safety Management System within the document, which

indicates the expected use. Table 5 summarises the expected use in the description column:

Table 5 List of techniques extracted from the NR SMS (Network Rail, 2018)

Technique	Description
Historical data analysis	Use of data to predict future outcomes
Visual data mapping	Mapping where risk areas are, using visual techniques such as coloured charts and maps
Hazard identification prompt lists	List of standard topics to be used in risk identification
Risk control prompts	List of standard controls
Structured What If Technique (SWIFT)	The Structured What If Technique is described as a team activity for the identification of hazards.
Hazard Log	A store for hazard information
Task Based Risk Assessments	A simplified technique that allows on-site operatives to undertake a rapid risk assessment before undertaking a task.
Interviews	A method of obtaining information about risks, normally from domain experts.
Hierarchical Task Analysis	A human factors analysis technique to break down tasks into stages and examine each element to assess risk.
HazOP	A formal risk identification technique for identifying hazards through a structured workshop process. It uses a set of keywords to guide the identification process. It is formally described in British standards.
Fault Tree Analysis (FTA)	This risk analysis technique provides a method of logically analysing the causes of a top-level safety event. Potentially, it can be used in a qualitative or quantitative mode. However, normally quantitative analysis is undertaken. It provides a method of carrying out a causal analysis. It is interesting to note that the SMS lists it primarily as a technique to identify root causes, which is not the case.
Event Tree Analysis (ETA)	This risk analysis technique is used to provide a logical analysis of the post

Technique	Description
	event consequences. Again, a qualitative or quantitative process can take place.
Cause consequence analysis	The SMS lists this as a combination of FTA and ETA, which is valid. However, this is a replica of the definition of the Bowtie method. It would have been more productive to describe it as a method that documents both the causes and the consequences of potential hazards. Normally, each hazard is listed in a table and the level of risk associated with each hazard is identified. Nominally this technique can be used to generate the basic information in a hazard record.
Common consequence tool	A bespoke risk analysis method of identifying locations where there is the potential for serious consequences in terms of train accidents. Locations are given a nominal score with a maximum value of 20.
Failure Modes and Effects Analysis (FMEA)	A risk analysis method of documenting the potential failure points of equipment leading to a failed intended operation and consequences.
Bow Tie Analysis	The risk analysis method is described as pivoted around a critical event. It is referred to as a structured method for cause consequence analysis.

The SMS defines 16 techniques in total; some are more applicable to system analysis than others. The list consists of a mixture of techniques for various stages, prompts, recording techniques, analysis techniques and bespoke tools.

All the techniques are assigned a category to indicate where they fit in the risk analysis process flow by the Author. The (CSM-REA, 2013) incorporates a description of the process stages. These are summarised as identification, analysis, evaluation, and recording of the risks. Implicitly, there is a requirement to treat the hazard if the level of risk is not acceptable. In addition, there is a

requirement to define the system under analysis before the process begins; however, for this categorisation, this can be considered an integral part of the identification process. A similar set of process stages are identified in the (Rail Safety and Standards Board, 2007). Therefore, it would appear that these are a sound basis for categorisation.

Some of the techniques listed are more tuned to a full engineering analysis than others. Another important category of risk assessments is the safe systems of work or Safe Methods Of Work (SMOW) which can be traced back to Section 2 of (HSAW Act, 1974) and is defined through case law by *Speed v Swift & Co* 1943 (SWARB, 2018). This is defined as a series of risk assessed steps written as a step-by-step process to carry out a task safely. It is created through a mini risk assessment process that goes through all the normal stages in a focused way. This research is not concerned with SMOW.

Table 6 shows the list of Network Rail techniques in a categorised form. These techniques form a substantial part of the reference list used in the industry survey of Chapter 4. The categorisation results influence the consideration of a new analysis technique by indicating the limitations of the current set of methods and whether the technique is an analysis method or not. For example, the Common consequence tool is bespoke to the Network Rail and therefore not generally accessible or applicable. In addition, the list of those identified as analysis methods is assessed for suitability for incorporation as part of the new technique in Chapter 6.

Table 6 Network Rail SMS risk techniques categorisation

Technique	Abbreviation	Bespoke to company	Applicability		SMOW	Process stage					Comments
			Specialist	General		Identification	Analysis	Evaluation	Recording	Treatment	
Historical data analysis				Yes		Yes					This technique is concerned with data mining from a large data set.
Visual data mapping				Yes					Yes		
Hazard identification prompt lists				Yes		Yes					
Risk control prompts				Yes		Yes					
Structured What if Technique	SWIFT			Yes		Yes					
Hazard Log				Yes					Yes		
Task Based Risk Assessments				Yes	Yes						Designed as a simple form to be filled in on-site to give an indication of the current risk.
Interviews				Yes		Yes					
Hierarchical Task Analysis			HF				Yes				Normally used by specialist human factors analysts.
HazOP				Yes		Yes					
Fault Tree Analysis	FTA			Yes			Yes				
Event Tree Analysis	ETA			Yes			Yes				

Technique	Abbreviation	Bespoke to company	Applicability		SMOW	Process stage					Comments
			Specialist	General		Identification	Analysis	Evaluation	Recording	Treatment	
Cause consequence analysis				Yes			Yes	Yes	Yes	Yes	
Common consequence tool		Yes					Yes				Used for modelling train derailments by assigning a risk number to locations
Failure Modes and Effects Analysis	FMEA			Yes			Yes				
Bow Tie Analysis				Yes			Yes		Yes		

3.2 Establish technique use

Currently, the precise methods used in practice by the industry for system risk analysis is unknown. It has been the Author's experience that very few of the available techniques have been used, although it is acknowledged that this may not be representative of the entire industry use. The methods that should be used are documented by various companies in their SMS and by RSSB. Therefore, it is desirable to survey practitioners with a list of recommended techniques to establish their usage.

Given that the railway is a geographically distributed undertaking with a large workforce and supplier base, an online survey is considered to be the most appropriate means of surveying a reasonable sample of practitioners. Kasunic (2005), pinpoints the importance of identifying the audience, and tailoring the survey to meet the expectations of the audience. In particular, the level of questions, language used and assumptions made. In this case, the target audience is professionals within the rail industry associated with conducting risk assessment work within companies carrying out change. The targets for the survey do not include regulatory personnel.

The industry is a large employer with Network Rail directly employing around 35,000, and the House of Commons committee for Exiting the EU (House of Commons, 2017) estimates that if all the suppliers and operators are considered it could easily reach a figure of the order of 225,000. A large number employed will be directly delivering customer service, ticket collectors, cleaners, drivers, for example, the estimated size of the potential target population for the survey

contracts from a potential of around 225,000 to something of the order of 5-10,000. Of this segment, a considerably smaller segment will be concerned with the execution of safety assurance as a specialist activity. Therefore, a non-parametric approach will be taken with the statistical analysis as advised by Krzanowski (1998) and Leven and Rubin (1998) where the sample size is potentially small and the distribution uncertain.

3.3 Appraisal of existing techniques

The list of techniques identified in Chapter 2 combined with those listed in the Network Rail SMS (Network Rail, 2018) provides a reasonably comprehensive list of existing techniques.

Trends in the literature have changed with risk analysis methods, as various interests come to the fore. Early analysis methods were mainly technological then interest grew in the effect of humans and the variability of their performance, while latterly there has been interest in the role of organisations. An analysis is undertaken by the Author to consider these points and their effect on risk analysis in a complex environment.

Methods have been categorised as either reflective or predictive in literature. A reflective method uses data from incidents and accidents to inform an expectation in a future system. An example is RSSB's Safety Risk Model; however, such a model cannot be applied to novel instances without modification. The term predictive appears to be superfluous in the context of an analysis. Grant, et al. (2018) reviewed what was termed five selected predictive risk assessment methods. The objective was to characterise them with 'tenets', to propose a

unified method in future. Other authors such as Underwood and Waterson (2013b) have carried out a comparison, in this case, from the perspective of usability. This analysis will draw on these tenets and usability criteria to comment and classify the methods.

As part of the analysis, the Author will provide a sense of the standing of the techniques qualitatively, by taking account of how well the methods satisfy the criteria. Consequently, this will enable the main and subsidiary research questions to be answered.

3.4 Review trends

Gathering data for test cases relies on documentation provided as a result of major accidents, because of public interest, these tend to be well documented and provide good well-reviewed material for analysis. There has been a period without serious accidents on the GB mainline railway that limits the amount of publicly available material to draw on for accident data from bodies such as RAIB.

However, the investigation reports that have been produced by RAIB over this period show themes that are at a lower level of Heinrich's (1932) risk pyramid as cited by Marshall, Hirmas and Singer (2018), where fatalities have been avoided. Nevertheless, these can still be subject to an analysis to reveal risk trends like whether systems have failed in isolation or a combined system has failed to function as expected.

3.5 Information gathering phase satisfaction of research questions

The main research question set out Chapter 1 will be addressed through a four-point approach described in at the beginning of this chapter as part of the information-gathering phase will address selected subsidiary research questions as shown

3.5.1 Technique use

The first approach has been developed into a survey. This survey will support the main research question and subsidiary question 2 in respect of:

- What methods are used today, and what are their particular features?
- Are current analysis methods in use suitable for the modern railway environment?
- What are the limitations of the current methods of risk assessment when applied to engineering projects?

Consequently, a view from the findings can be taken on the current state of risk assessment and therefore provide indicators about the required properties of possible new method. By considering

- How can the current risk analysis methodologies be amended to create a generically applicable method in a usable way without the requirement for expert knowledge?

through opinion-based survey questions an answer to supporting question 1 could be forthcoming. As part of understanding how to combine and express risk as required by subsidiary question 1 a consideration of

- How should the variables that affect risk be weighed?

can also be investigated through further opinion-based survey questions. These particular questions will provide an opportunity to assess how the industry complies with the legal requirements as well as which set of legal requirements form the primary basis for risk acceptance, those with roots in Europe or those with roots in (HSAW Act, 1974).

3.5.2 Appraise existing techniques

The second approach is a desktop review using available material. The appraisal will support the satisfaction of the main research question by indicating:

- If current analysis methods suitable for the modern railway environment
- The limitations of the current methods of risk assessment when applied to engineering projects
- The advantages and disadvantages of quantitative and qualitative risk assessments

Commentary with the support of the categorisation of the methods will support the provision of the required information and thereby contribute to the satisfaction of subsidiary question 1 by indicating the strengths and weaknesses of the quantitative and qualitative techniques.

3.5.3 Review of trends

The third approach has been developed into a desktop review of the RAIB dataset. This will address the main research question and subsidiary research question 2 by identifying:

- What are the characteristics of the recorded incidents
- If current incidents involve multiple subsystems or parts

Implicitly the answers will provide inputs to subsidiary question 2 and enable an answer to be produced about the detection requirements. The data provided through the review will indicate areas where incidents have occurred and whether a failure is of a complex system composed of multiple parts rather than isolated equipment. A cluster of incidents of a particular type will indicate a possible weakness, while a statement of the opposite effect will not be possible. The data

will indicate the attributes required from a new method and contribute to answering the main research question.

3.6 Summary

This chapter has developed the four-point approach of chapter 1 into an online survey to gauge the use of current analysis techniques. Moreover, an appraisal of current techniques is to be undertaken to identify the features and limitations for risk assessment. Furthermore, trends of incidents are to be investigated by reviewing RAIB data to reveal if incidents are single or multisystem events. The research methods described are used in Chapter 4 and Chapter 5 to obtain data to use to weigh the need for a new method. Furthermore, the data will guide the features a new method requires.

3.7 Principal points

The principal points from this chapter are as follows:

- i. A four-point approach is used to investigate risk assessment in the railway environment.
- ii. Compliance with the SMS is a legal requirement.
- iii. Expecting the risk assessment techniques listed in the SMS's to be used by the industry is a valid expectation.
- iv. The Network Rail SMS is used starting point to identify techniques that should be in use in the rail industry

- v. The risk assessment techniques are aligned to the CSM risk assessment stages
- vi. The industry survey applies to a small sample because risk analysis is a specialist activity
- vii. The current methods are to be examined by the Author using predetermined categories from the literature review
- viii. Using RAIB data is valid even though there have been few public fatalities and characterisations of incidents are representative.
- ix. The main research question and the two subsidiary research questions are addressed by the developed research methods.

4 Current methods appraisal, survey and results

Chapter 3 developed an approach and justified the research methods to be used, this chapter uses the methods to gather information. It reports on the implementation of a railway industry survey and a desktop appraisal of the current methods features, strengths and weaknesses.

4.1 Survey

As described in Chapter 3, Section 3.2, an online survey has been developed with a target audience of safety professionals and those associated with safety decision making. Roles specifically identified forming part of the target audience were:

- Safety engineers
- Project managers
- Designers
- Assessor contractors

4.1.1 Development

The survey was developed and reported (Barnatt, 2019a) using techniques described by Dunleavy (2003), McCormack and Hill (1997) and Kasunic (2005) and summarised in the following paragraphs.

After reviewing the research questions, an objective was set to satisfy the research questions by supporting the following:

1 What methods are used today, and what particular methods are used for any specified project type?

2 Are current analysis methods in use suitable for the complex modern railway environment?

3 What are the limitations of the current methods of risk assessment when applied to engineering projects?

Figure 4 depicts the ten sectors identified from the audience analysis.



Figure 4 initial survey sectors (Barnatt, 2019a)

The potential audience size was estimated as described in Chapter 3. The university ethics process approved the proposal for the survey. An examination of the questions was carried out during the development to consider the expected range of answers and make certain that the objectives for the survey would be met.

The survey was piloted, and an unpublished report was produced (Barnatt, 2019b). The feedback anticipated an 85% completion rate. It also contained three specific comments on the length of two questions and wording. The eventual survey distributed to the industry contained the changes from the feedback.

4.1.2 Conduct and interpretation

The anonymous survey was conducted through the online SurveyMonkey tool between 4 July and 4 August 2019 via an invitation shown in Appendix A. One hundred twenty-six invitations were sent out to a pseudo random¹¹ selection of the target audience, and 30 valid responses were received, a response rate of 24%. Unfortunately, a further nine invalid responses were also received and discarded, with a significant number of unanswered questions that were put down to internet connection problems.

The number of responses will affect the confidence level and precision of the survey. Kasunic (2005) provides a formula to estimate these parameters. The confidence level has been set at 90% to assure that the sample is valid and will remain within the calculated precision for the survey nine times out of ten.

However, with 30 valid responses, the precision has dropped to 79%, indicating that the survey will not represent the population a fifth of the time. Therefore, it is reasonable to conclude that while the survey is not definitive, it provides indicators of industry trends.

As Kasunic (2005) recommended, in the case of questions intended to identify a sector, non-responses will be allotted to an 'undefined' category to avoid bias through an arbitrary assignment. Furthermore, where multiple answer questions were partially answered, these have been designated as valid, and the respondent population was reduced for that element. It has been assumed in this case, the respondent is either unsure or has no opinion.

¹¹ Invitations were sent to the members of the RSSB subject committees with requests to forward them to relevant engineers within their constituency/companies. This was supplemented by further requests where a few committee members were uncontactable. The initial selection ensured industry representation and the forwarding created a level of randomisation.

Questions 4 and 5 that probed the respondent's understanding of the methods including less well-known ones such as FRAM; consequently, occasional non-responses were not unexpected and does not undermine the results.

The questions are reproduced in Appendix A. Questions 1 and 2 were intended to indicate the respondent's sector and type of work. The objective is to use this as a selection parameter to identify differing practices in various parts of the industry.

Questions 3 and 4 were designed to indicate the understanding of various techniques and their use; while question 5 is used as a cross-check of technique understanding.

The survey was designed to indicate whether there is a knowledge gap concerning the techniques available. If there is a high correlation between the use and understanding questions, it would indicate no knowledge gap.

The list of methods contained in the questions was extracted from those contained in this thesis, the Network Rail SMS (Network Rail, 2018) chapter on risk assessment, supplemented with additional methods identified from the literature review in Chapter 2. The list has been converted into risk assessment stages aligned to those outlined in the CSM process (CSM-REA, 2013) and Rail Safety and Standards Board (2007).

Table 7 Risk assessment stage definition

Stage	Description
Identification	Identification of the hazards
Analysis	Assessment of the level of risk, causes and consequences
Evaluation	Comparison of the risk level with norms for acceptability
Recording	Recording of the risk data in a formal record

Treatment	Further risk mitigation treatment to reduce the level of risk
-----------	---

The technique risk assessment stage assignment established from Chapter 3 is given in Table 8

Table 8 Risk assessment stage assignment

Technique	Risk assessment stage					Comments
	Identification	Analysis	Evaluation	Recording	Treatment	
Historical data analysis	Yes					
Visual data mapping		Yes				
Hazard identification prompt lists	Yes					
Risk control prompts		Yes				
Structured What If Technique (SWIFT)	Yes					
Hazard Log				Yes		
Task Based Risk Assessments	Yes	Yes	Yes	Yes	Yes	Designed as a simple form to be filled in on-site to give an indication of the current risk and contains all stages as a mini total process
Interviews	Yes					
Hierarchical Task Analysis		Yes				
Hazard and Operability (HazOP)	Yes					
Fault Tree Analysis (FTA)		Yes				
Event Tree Analysis (ETA)		Yes				
Cause consequence analysis		Yes	Yes		Yes	
Common consequence tool		Yes				Used for modelling train derailments by assigning a risk number to locations
Failure Modes and Effects Analysis (FMEA)		Yes				
Failure Modes Effects and Criticality Analysis (FMECA)		Yes				

Technique	Risk assessment stage					Comments
	Identification	Analysis	Evaluation	Recording	Treatment	
Bow Tie Analysis		Yes				
Swiss Cheese Model		Yes				
Functional Resonance Analysis Method (FRAM)		Yes				
STAMP		Yes				
Code of practice compliance			Yes		Yes	
Reference system comparison			Yes			
Formal methods		Yes				

Following on from the discussion on questions 1 to 5 above; questions 6, 7,8 and 9 were designed to indicate whether assessments are currently undertaken in isolation or whether there is a more holistic systems approach. Finally, question 10 was designed to elicit a social attitudes response to how risk is assessed and which versions of legislation respondents considered important.

4.1.3 Results

This section reports the results of the survey. It provides an analysis describing the results in the context of the thesis and where appropriate drawing inferences.

The surveys were sent to the target audience sectors, as shown.

Survey sector distribution

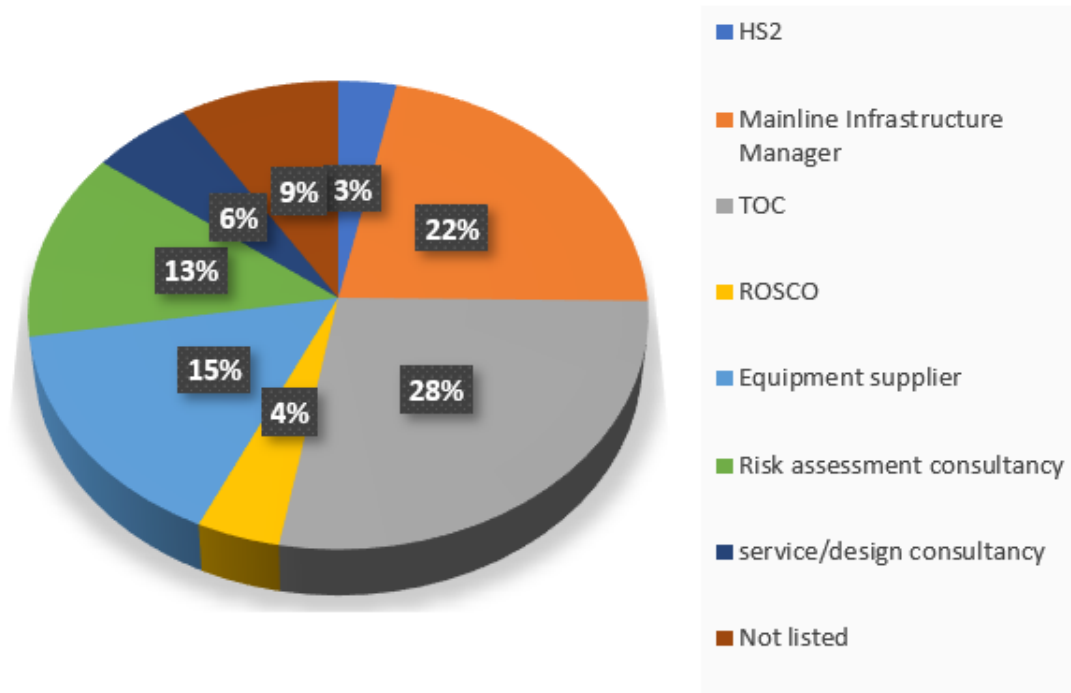


Figure 5 surveyed sector distribution

As can be seen, the survey was sent to a large number of infrastructure managers and TOCs, reflecting their dominance of the industry in terms of employees. The sector-by-sector response was as shown:

Sector response

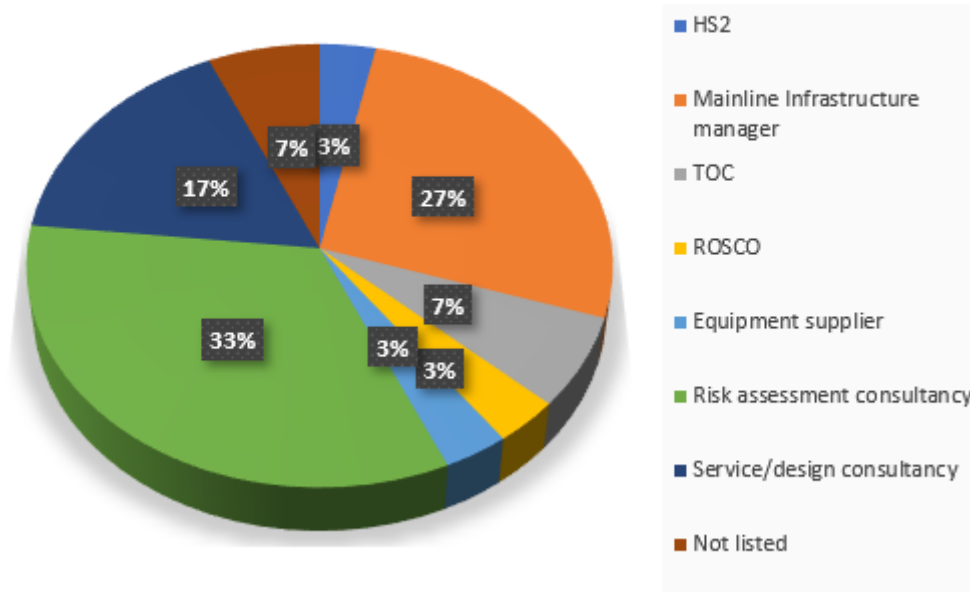


Figure 6 survey sector response

As can be seen from Figure 6, respondents are mainly from infrastructure managers or consultancies, with others from the train operating community. A review of industry websites indicates that the consultancy industry is geared up to support the industry need and exemplified by Aegis Engineering (2019) and Ricardo Rail (2019) where assurance and vehicle services feature heavily. Also, when trains are supplied, they are required to comply with European legislation (RIR, 2011) regulation 4, therefore manufacturers are likely to be obliged to undertake the assessment work before supply, either doing it themselves or engaging consultancies. In contrast, the higher response from infrastructure managers may be explained by the constant requirement to provide a safety assessment. Furthermore, these sectors represent large companies which are well resourced and therefore can sustain an in-house capability which may not be the case for train operators. Therefore, the Author concludes that the data set is

reasonably representative of both the infrastructure assessments and vehicle assessments.

4.1.3.1 Method understanding

Question 3 probed the understanding of the current methods. There were six classifications where Not Aware, Aware, and Basic are considered as indications that the technique is not used in practice by the respondent. The question was stated as:

“Please indicate your level of understanding of the following risk assessment techniques”

The methods listed in the question included those newer methods, which are classed as:

- Functional Resonance Analysis Method (FRAM)
- STAMP

It was found that 69% of respondents were not aware of FRAM, and 55% were not aware of STAMP, while 14% and 31% were only aware of the techniques. This finding supports the assertion of Salmon, Cornelissen and Trotter (2012) that STAMP is not popular.

Formal Methods were found to have a low level of understanding, with 48% of respondents either unaware or aware of the method and a further 30% of respondents having a basic understanding. This response indicates that this technique is not in mainstream use.

All of the respondents were aware of the two CSM methods explicitly contained in the list:

- Code of practice compliance
- Reference system comparison

The respondents indicated that 83% and 72% considered themselves at least proficient, suggesting that these techniques are widely used in the industry.

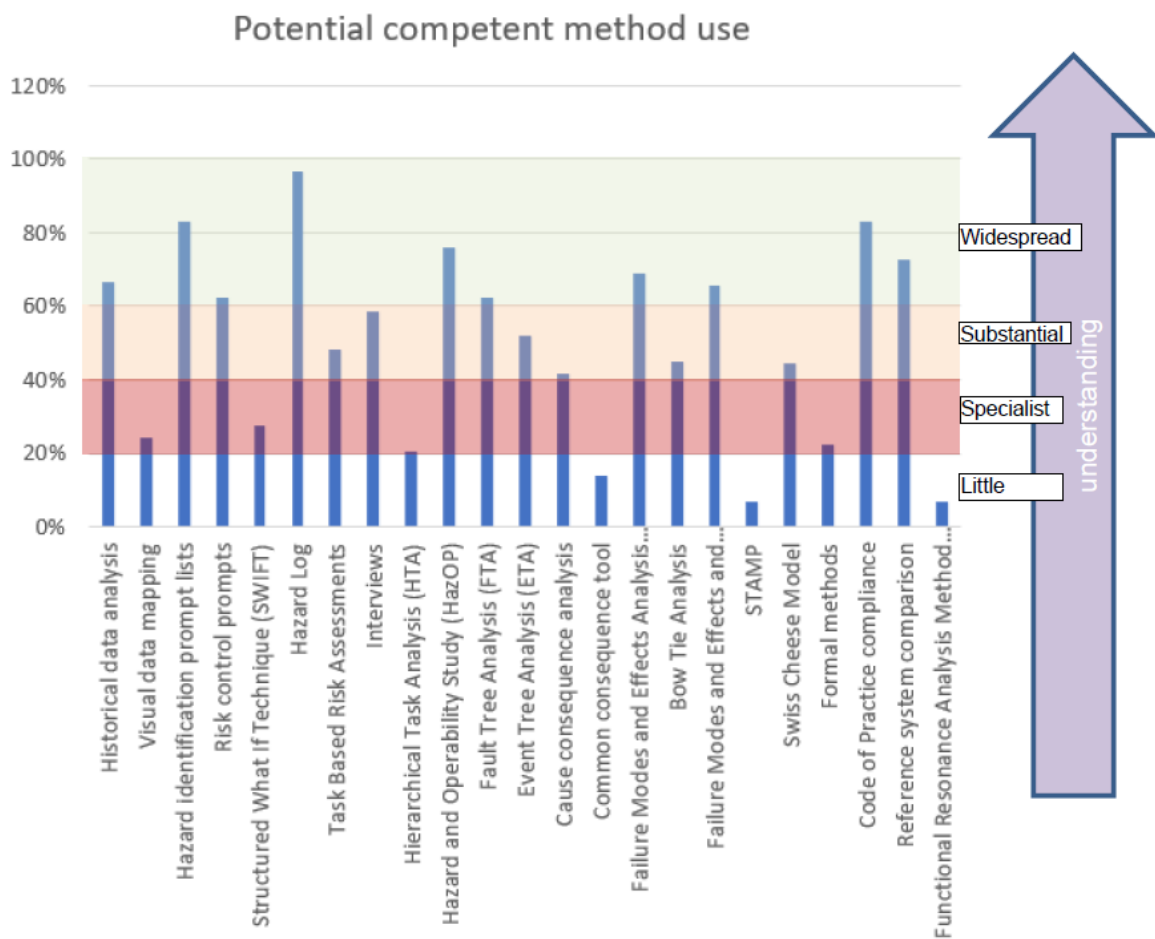


Figure 7 Potential competent method use -processed question 3 data

Table 9 Potential competent method use

Level of understanding	Technique
Widespread	Historical data analysis Hazard identification prompt lists Risk control prompts Hazard log Hazard and operability study (HazOP) Fault tree analysis (FTA) Failure modes and effect analysis (FMEA) Failure modes and effect and criticality analysis (FMECA) Code of practice compliance Reference system comparison
Substantial	Task based risk assessments Interviews Event tree analysis (ETA) Cause consequence analysis Bow tie analysis Swiss cheese model
Specialist	Visual data mapping Structured what if technique (SWIFT) Hierarchical task analysis (HTA) Formal methods
Little	Common consequence tool STAMP Functional resonance analysis method (FRAM)

From an inspection of Figure 7, it appears that there four groupings of the potential use of methods, defined as methods where the respondent indicated at least a proficient level of understanding, implicitly indicating some level of

experience. Table 9 tabulates these for clarity. Figure 7 shows the first group of techniques that have a wide level of understanding where 60% or more of respondents are rated as at least proficient. Second, a group of methods between 40% and 59%, indicating a substantial level of understanding. The third group of methods between 20% and 39% that include more specialist techniques such as HTA and formal methods where it can be expected that there is a smaller level of use by a specialist community. Finally, the fourth group below 20%, indicating little understanding and consequently the potential for use. As expected, these include FRAM, STAMP and the Network Rail specific common cause tool.

A surprising finding from Figure 7 is that the SWIFT method has a low rating given that it is a simple technique and is a more flexible version of the HazOP method which is understood by 76% of respondents. This finding may indicate that it is not enough to provide a simple method; it must also achieve a level of following to be taken notice of.

Figure 7 clearly shows a finding that FMEA and its variant FMECA are the most understood analysis techniques followed by FTA and ETA. All of these are traditional techniques that have been criticised by writers advancing their 'modern' techniques such as Leveson (2011). It appears from these findings that the industry is content with these traditional techniques and that the authors of the 'modern' techniques have failed to carry the industry with them.

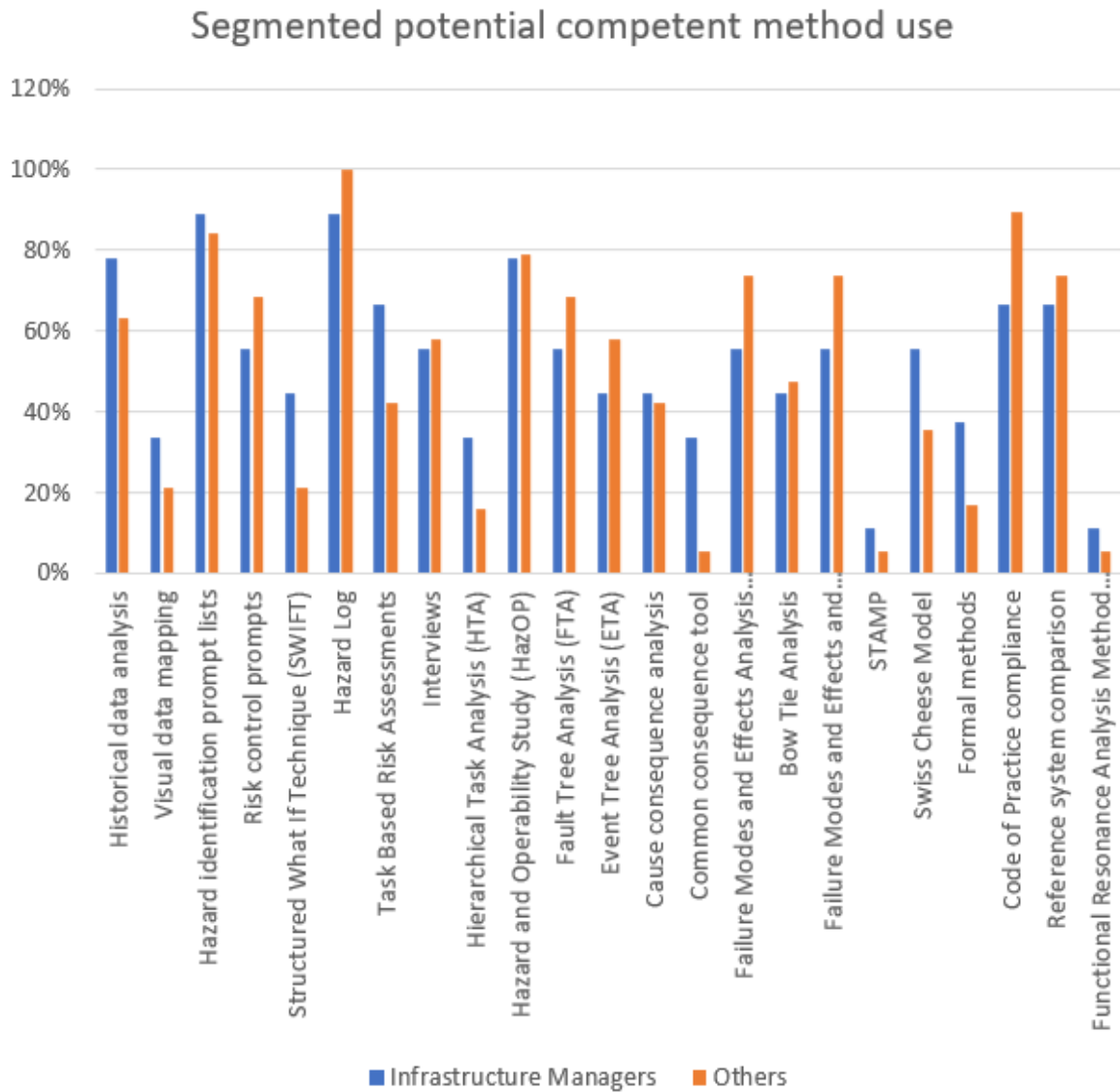


Figure 8 Potential Method use by infrastructure and other segments

The values shown in Figure 8, were subjected to a standard paired Wilcoxon signed-rank test, which is a non-parametric test to detect the difference in means between two samples. The method uses a Tvalue to denote a critical point which is compared with a calculated value, values above this indicate that there is no statistical significance. In this case, the statistical method is to test if there is any difference in the understanding between the two groups (infrastructure managers and others). The hypothesis is:

- Ho There is no overall difference in the level of understanding of assessment methods between the Infrastructure Managers and others.
- Ha There is a difference in the level of understanding of assessment methods between the Infrastructure Managers and others.

The critical value selected from tables, (University of Calgary, unknown), for an alpha level of 0.05 two-tailed test is 73. The calculated Tvalue is 113, and therefore, Ho is accepted, and it is concluded there is no substantive difference in understanding between the groups.

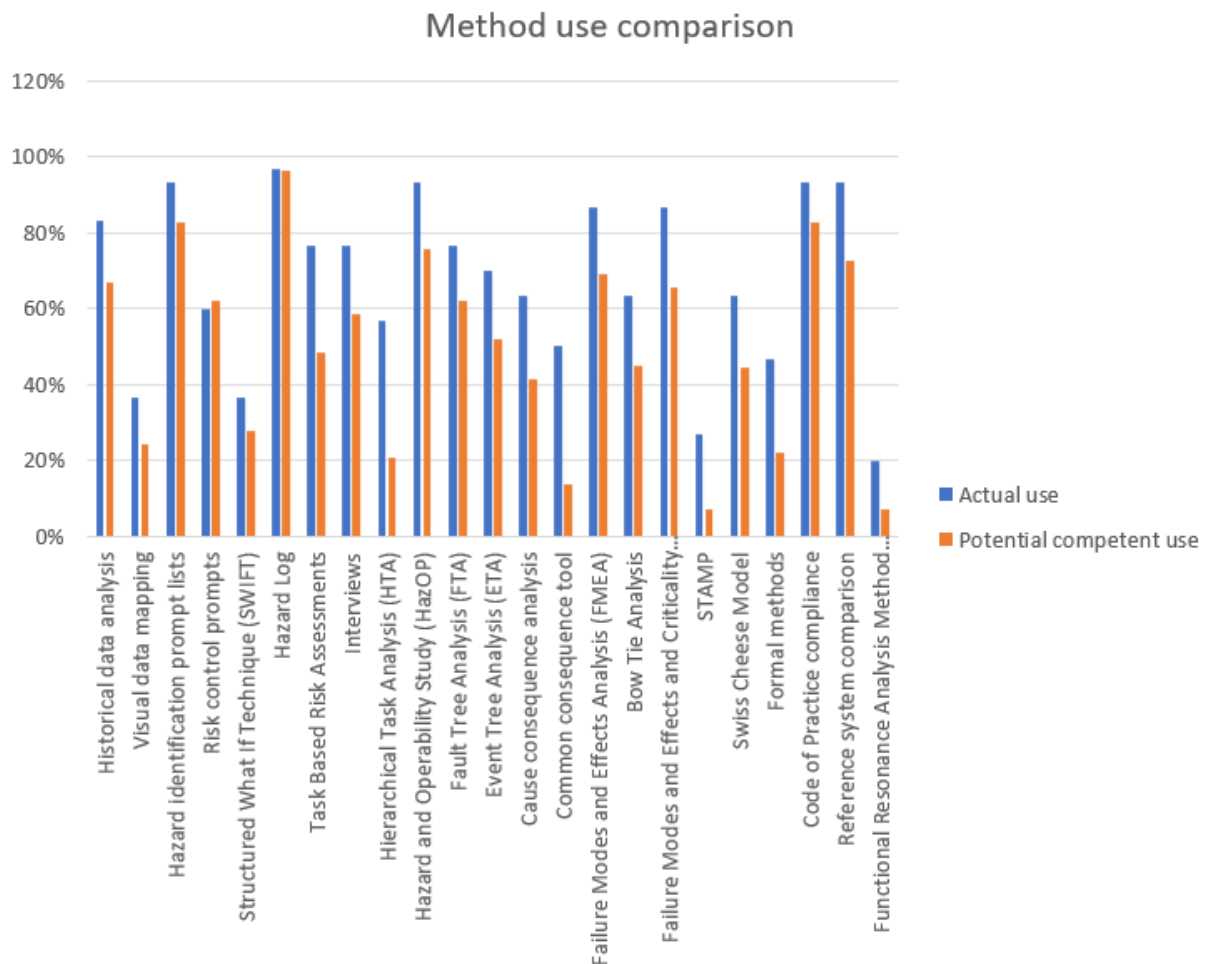


Figure 9 Method use comparison

Figure 9, indicates the responses from questions 3 and 4, which were stated as:

“3. Please indicate your level of understanding of the following risk assessment techniques”

“4. Please select and rank the risk analysis techniques used by you or know to be used by your team in order of preference of use (1 being the most preferred technique)”

Question 4 invites respondents to rank the methods they use and indicate those that were not used through a checkbox. Logically, the techniques where the checkbox was selected should be those that align with the techniques where the respondent was not assessed as competent. If this were the case, it would imply that respondents only use the methods when they are competent. The blue bars denote the responses where respondents have indicated they use the technique in practice. Since the blue (use) bars are higher than the orange (competence) bars in Figure 9, it would suggest there is some use of some techniques by those who are not proficient which may lead to a varying quality of assessment. An alternative explanation is they are used by colleagues who are specialists. Applying the Wilcoxon signed-rank test non-parametric test, explained above, to detect if the two sets of data are statistically different. The hypothesis is:

- H_0 There is no overall difference between the techniques in use and those that are understood.
- H_a There is a difference between the techniques in use and those that are understood.

The critical value selected from tables, (University of Calgary, unknown), for an alpha level of 0.05 two tailed-test is 66. The calculated Tvalue is 1, and therefore

Ha is accepted, indicating there is a substantive difference, and the suggestion is statistically significant.

The findings from question 5 indicate that there is some uncertainty about which stage of the process a particular technique should be used. The percentage of respondents indicates this uncertainty.

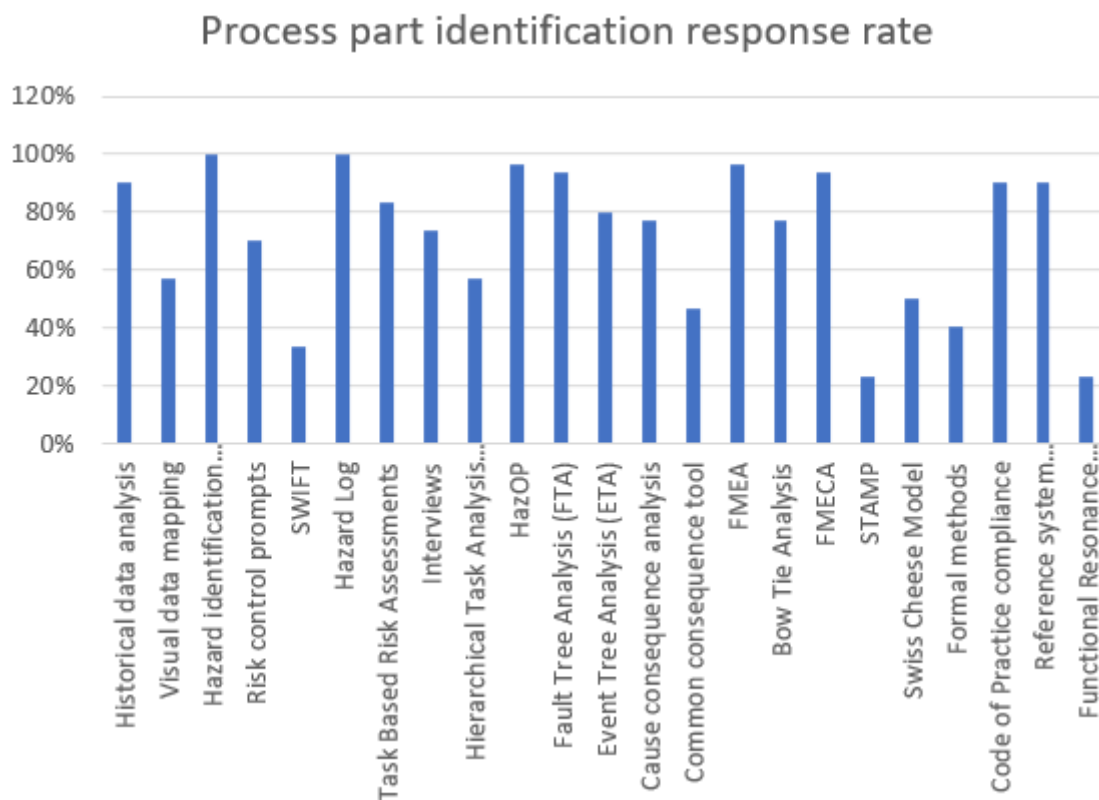


Figure 10 Percentage of respondent allocating a method to an assessment stage

Figure 10 indicates a similar picture to the previous responses.

The findings suggest that there is a widespread reasonable understanding of the ‘traditional’ methods, while there are some methods where there is a smaller specialist group and the newer methods are not understood. It has been found that the FMEA based methods are the most popular form of analysis, while HazOp

and prompt list are the most recognised identification method, and the hazard log is the most recognised recording method.

The presentation of data from question 5 in Figure 11 is as a series of histograms. The expected technique type assignments are denoted by green bars, which are taken from Table 8. Respondents were permitted to assign a technique in any number of stages. Therefore, a respondent who felt that a technique played a part in all the stages of the risk assessment process could select all the stages.

Conversely, if a respondent felt it did not apply to any stages could equally select none of the stages.

The percentages in the charts represent the percentage of respondents who selected the technique, selecting that stage. For example, taking the 'Identification' stage, the HazOp method was selected for this stage 93% of the time by respondents who selected the HazOp method. As can be seen, there is a variance with the assignment set out in Table 8, which is derived from Chapter 3. For every stage, except for 'Evaluation', at least one of the expected methods was more popular than unexpected methods. The graphs suggest there are some alternative views of the function of some techniques, with significant proportions of the population assigned to alternative stages. This result confirms there is some confusion over the actual use of the various methods with respect to the expected use. From a positive perspective, the findings show that techniques selected for the identification, analysis and recording stages attracted some 80% and over for the expected assignment. Notably, HazOPs are almost universally recognised as an identification tool and hazard logs as a recording device.

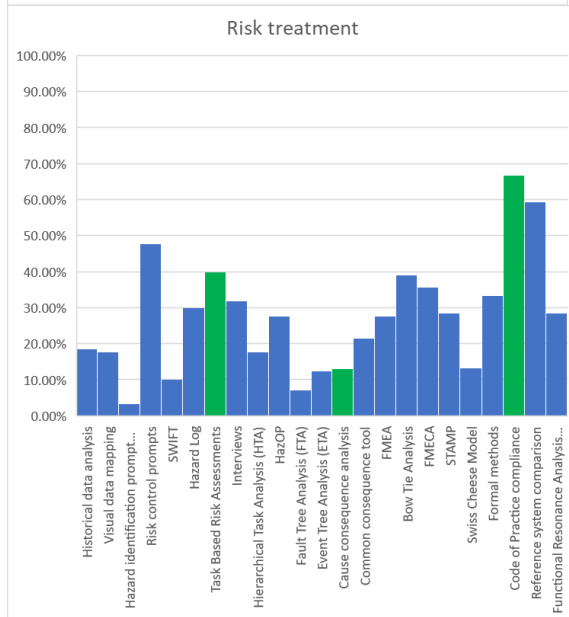
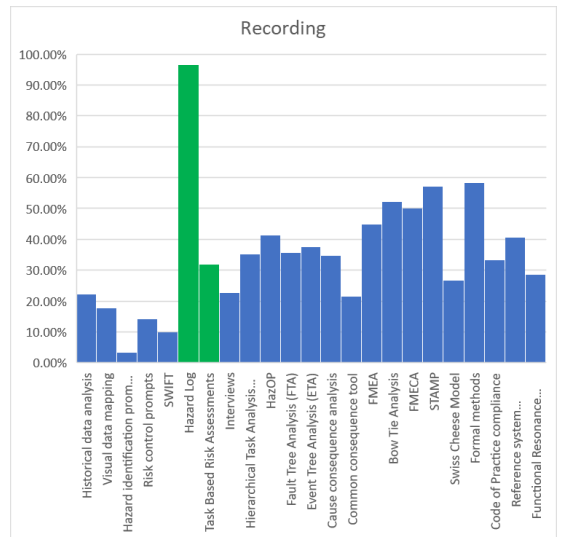
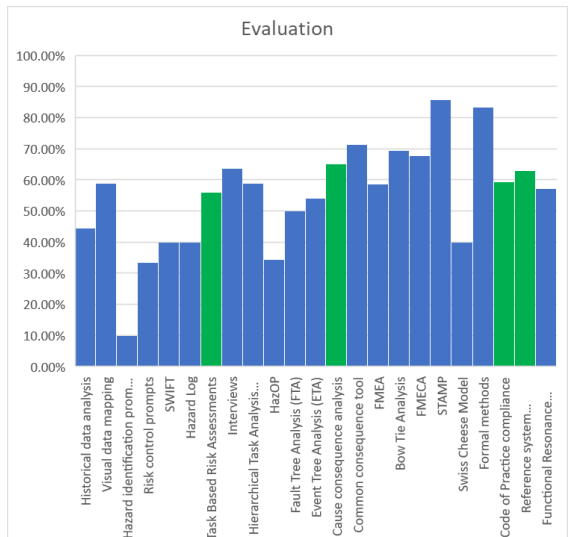
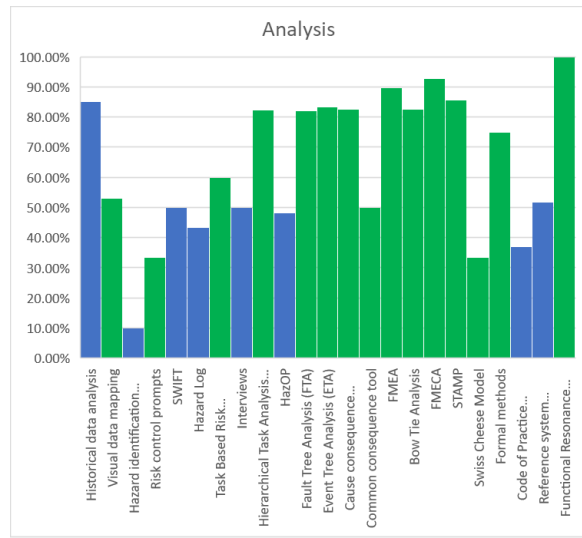
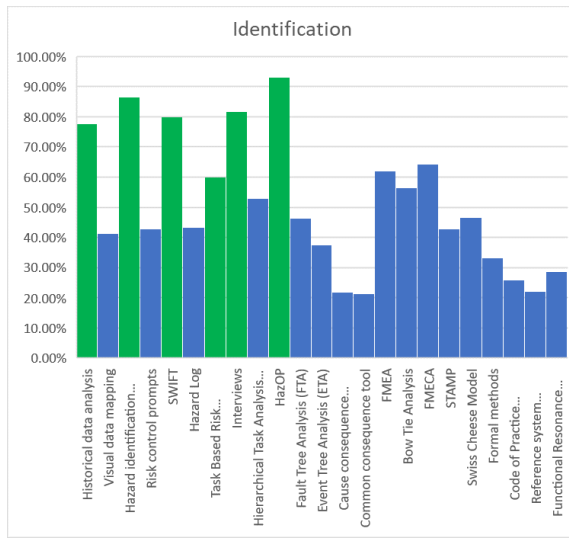


Figure 11 method assignment to process stage

The evaluation stage does not appear to have been understood. Respondents have selected analysis techniques, such as FMEA, or identification methods, such as risk prompts, rather than those that meet the evaluation requirement specified (CSM-REA, 2013). Alternatively, it may indicate that respondents took a much broader definition of evaluation and interpreted it as the act of analysing risks or identifying risks. Nevertheless, it is significant that this is the only stage where an alignment with at least one of the predefined methods does not occur. It is also interesting to note that the two European methods of reference systems and codes of practice are strongly identified as risk treatment and evaluation even though the reference systems do not provide treatment. Overall, the results indicate a measure of understanding of the process's identification, analysis and recording stages, but there is less understanding of the evaluation and risk treatment stages.

A comparison of the results with the derived assignments is shown in Table 8 is given in Table 10. As can be seen, the percentage of respondents allocating the technique to the same stage as the derived assignments is shown in the stage cells.

Table 10 Percentage of respondents assigning the technique to the assigned risk assessment stage

Technique	Risk assessment stage				
	Identification	Analysis	Evaluation	Recording	Treatment
Historical data analysis	70				
Visual data mapping		30			
Hazard identification prompt lists	87				

Technique	Risk assessment stage				
	Identification	Analysis	Evaluation	Recording	Treatment
Risk control prompts		23			
Structured What If Technique (SWIFT)	27				
Hazard Log				97	
Task Based Risk Assessments	50	50	47	27	33
Interviews	60				
Hierarchical Task Analysis		47			
Hazard and Operability (HazOP)	90				
Fault Tree Analysis (FTA)		77			
Event Tree Analysis (ETA)		67			
Cause consequence analysis		63	50		10
Common consequence tool		23			
Failure Modes and Effects Analysis (FMEA)		87			
Failure Modes Effects and Criticality Analysis (FMECA)		87			
Bow Tie Analysis		63			
Swiss Cheese Model		17			
Functional Resonance Analysis Method (FRAM)		23			
STAMP		20			
Code of practice compliance			53		60
Reference system comparison			57		
Formal methods		30			

Table 10 bears out the findings from Figure 11 that there is less alignment with the derived stage assignment for the evaluation and treatment stages. It is worth noting that the Swiss Cheese model is not seen as an analysis tool by over two-thirds of respondents, despite Reason's texts Reason (1997) and (2016). This result may be reflective of the SCM being a high-level tool at first glance, but as Underwood and Waterson (2013b) has shown it is used successfully in air accident investigation. Furthermore, it reinforces the view the established analysis

techniques such as FMEA are well understood, while the new methods, STAMP and FRAM, are not well understood or widely used.

4.1.3.2 Systems approach

Questions 6 to 9 are designed to find insights into the approach to systems and whether assessments are undertaken in isolation.

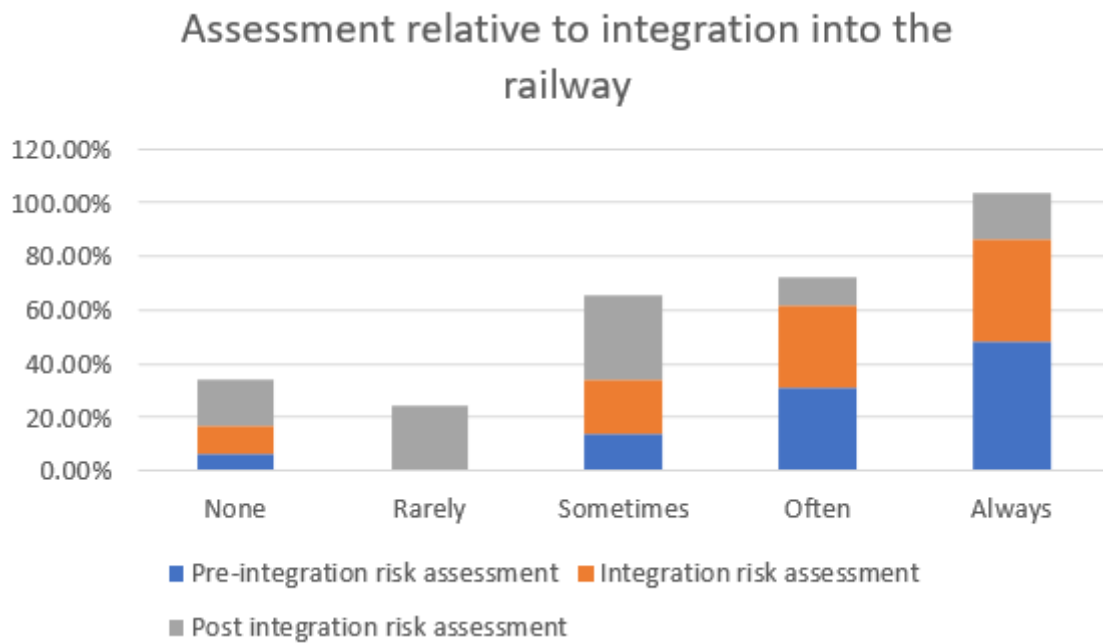


Figure 12 Assessment approach concerning integration

Figure 12 suggests that the dominant approach is to perform the assessment before integration, which indicates that a substantial amount of assessment is still carried out in isolation. Likewise, there is a significant segment of assessment at the time of integration. Conversely, post-integration assessment is far less popular. Respondents were also requested to indicate to what extent they considered the external environment when carrying out an assessment when answering question 7, and the average value was 72%. Question 8 requested that respondents indicate if they carried out assessments for specific targeted systems or on a more generic level, and it was found that 89% assessed for specific

targets. Overall, this would suggest that methods need to incorporate an isolated assessment approach with the capability of being able to summarise the overall system-level effect, including the effect on the environment.

Question 9 did not provide any substantive indications of trends about whether assessments were carried out in parts and combined or the system is considered as a whole. As a result, this is not considered a key parameter in the approach to assessments.

4.1.3.3 Attitude to risk assessment

Question 10 tests the attitudes toward risk assessment, where respondents were requested to indicate the level of alignment with their strategy and methods.

Figure 13 shows, unsurprisingly, there is a strong indication of alignment, 76% of respondents, with the concept of As Low As Reasonably Practicable because it aligns with HSAW.

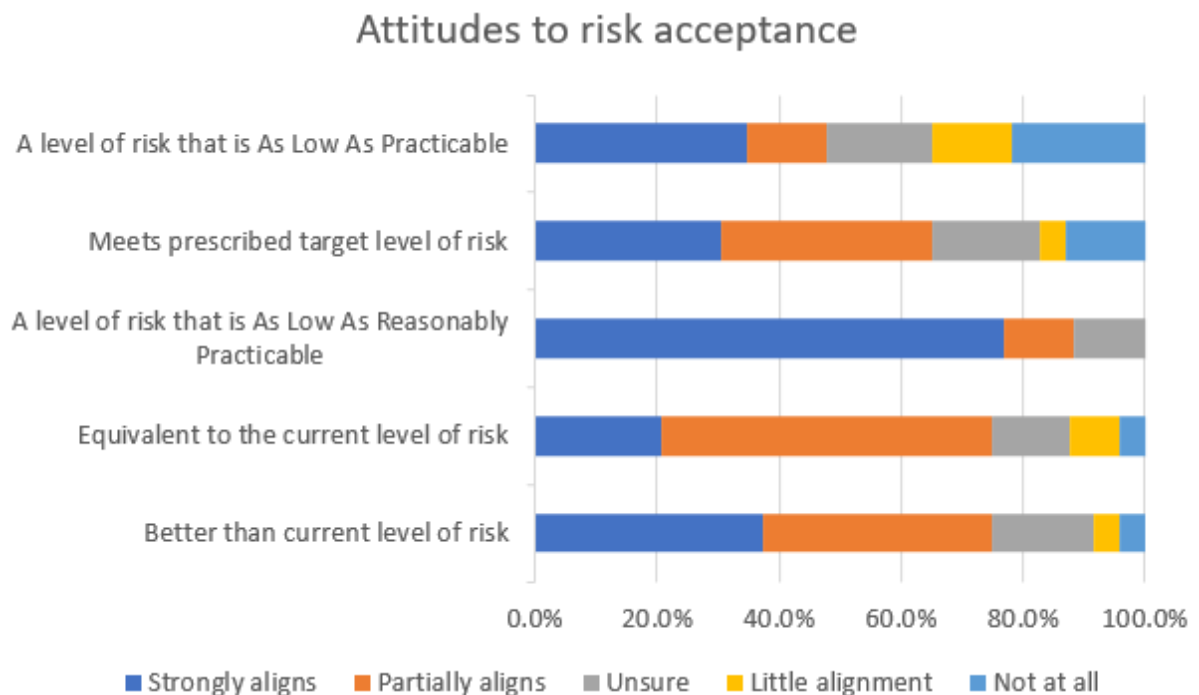


Figure 13 Bar table of attitudes to risk acceptance

What is more surprising is that the “equivalent level of risk” category does not have a similar score given it is equivalent to the CSM reference system evaluation method, which was indicated as being widely understood earlier. This category scores 21% indicating strong alignment, while 54% indicate partial alignment. Similar comments are attributed to the “meets prescribed target level of risk” category; however, there appears to be a slightly higher recognition of alignment with 30% of respondents indicating a strong alignment. The near 40% strong alignment indication for the As Low As Practicable category, indicates a lack of understanding of the legal position because effectively that means doing everything possible, without limit; something no business is able to commit to.

It is notable that with the advent of CSM and Interoperability that there is such a strong indication of alignment, 38% with the “better than current level of risk”. Although this is laudable as an objective, there is no legal requirement to do so. The sentiment may be more due to commercial pressures driven by a need to be seen as improving.

Overall, this appears to indicate there is some misunderstanding of the risk acceptance criteria required by law.

4.1.4 Finding conclusions

In summary, the evidence demonstrates a much better familiarity with traditional risk assessment practices, as described in section 4.1.3.1. There is a dominance of risk assessment prior to integration, described in section 4.1.3.2, followed by an assessment at the time of integration. These findings imply that any successful method must be able to integrate both approaches. Likewise, there is more alignment of risk acceptance criteria with the traditional As Low As Reasonably

Practicable than the newer requirements from the CSM regulations. There appears to be a reasonable understanding of what the identification, analysis and recording stages of a risk assessment require, but much less of an understanding of the evaluation and mitigation (treatment) stages. It would appear that it would be an advantage to integrate these stages into the process and mask them from the user, which effectively is done through the cause-consequence tables aligning with the legal requirements, as described in Chapter 2. Therefore, it would be beneficial for a process to be compatible with the cause-consequence method.

4.2 Current methods appraisal

The section describes an assessment undertaken by the Author to gauge attributes, strengths and weaknesses of risk analysis methods which will provide indications of where a new method could advance the state of the art.

The term “Current methods” refers to current risk analysis methods. It is often not clear what is meant by a risk analysis method within the literature and in practice, as has been shown in Chapter 3, Section 3.1. In this section, it means a process or collection of processes taken together that can express safety risk, where risk is an expression of likelihood and consequence. In addition, the methods should be able to express the level of risk in some form.

Methods have been categorised as either reflective or predictive in literature, as described in Chapter 3 Section 3.3. Categories have been extracted from Grant, et al. (2018) which were described as ‘tenets’, to propose a unified method in future. Other authors such as Underwood and Waterson (2013b) have also carried out a comparison in this case from the perspective of usability and found that newer methods such as STAMP from Leveson (2011) have low uptake and in effect are

not practical. The Author has developed a set of classifications using these insights, to highlight what are considered key themes for risk analysis methods as described in Table 11.

Table 11 Definition of classifications

Classification	Description and rationale
Category	A method referring to a technique as of a particular class.
Focus	The aspect that a method will emphasise. For example, the method could consider human factors.
App	Application of the technique to either an accident analysis or design.
Model	This attribute indicates the type of model that is used within the method. It is intended to indicate the level of realism required by the method.
Division	This attribute indicates the basis used to decompose the various parts in the analysis. Some methods do not explicitly include a decomposition method. It is then left to the user to use experience and knowledge to perform the task; this is the case with the older, more established models.
Scale	These are a measure of how the risks are scaled. These could be word, value-based or numerical. Dependent on the application, there are advantages and drawbacks to each. For example, a numerical approach might indicate improvements which are not realisable due to the uncertainties in measurement.
Start	The point at which the analysis is expected to begin.
Documented	The medium that is used to document the analysis which could be words or pictorial. These approaches are suited to different types of analysis. For example, a pictorial approach is a good medium to show an overall sense of an analysis. While, it could be the case that this is done at the expense of detail, where a word-based technique would come to the fore.

Identification of key attributes is crucial to assessing the benefits and limitations of risk assessment methods, and these are set out in Table 12. As noted by Grant, et al. (2018), this is not easy because of the different terminology and points of reference taken by authors. Where appropriate, attributes have been grouped together into classifications, these represent different aspects of a theme that

facilitate a clearer analysis. Classification of the 'focus' is based on that used by Hollnagel (2012) for the analysis framework. It is regarded as a primary discriminator for the analysis. Table 13 below has been constructed using attributes to identify the features of the various techniques. These have been assessed qualitatively by weighing benefits and limitations to provide a measure of qualities as part of this research, taking account of personal experience and comments from the various literature cited in Chapter 2.

Table 12 Definition of attributes (reformulated from sources cited in Chapter 2)

Attribute	Classification	Description
Traditional	Category	An established technique that has been in use over several decades. Typically has a technical focus
Sociotechnical	Category	A newer technique the integrates technical, human factors and organisational aspects. Typically has a focus on human factors and organisational aspects. In addition, it will provide a detail of the hierarchy of control
Other	Category	Those techniques that do not fit into the other two categories. Typically, these include new technically focused methods and modelling methods.
Technical	Focus	Technical aspects are taken into account and drive the analysis. Typically, equipment is analysed for function.
Human factors	Focus	Operations performed by people, groups of people, drive the analysis. Within this group is the consideration of human error and user interfaces. In addition, procedures are taken into account where reliance is placed on operators.
Organisational	Focus	The effects of the structure of the organisation and how it interacts with its environment drive the analysis.
Retrospective	App	Aimed at analysing accidents. There is normally an event and causes are then deduced.
Predictive	App	Aimed at the prediction of the behaviour of a system. The technique could also be used to analyse accidents by the application of deduction.
Specialist application	<i>None</i>	The method is aimed at a particular aspect of risk analysis.

Attribute	Classification	Description
Historic data	<i>None</i>	The analysis method relies on the use of data gathered from previous events to predict future outcomes.
Conceptual	Model	The analysis method provides a model where a general concept can be applied to obtain an overall understanding. An example of this approach is the Swiss Cheese Model.
Abstract	Model	The instance being modelled is framed around an abstract concept, such as a hierarchy linked to an operational system, as is the case with STAMP.
Instance-based	Model	The model is specifically created for the instance under analysis. Therefore, each application will have to be modelled from scratch.
Hierarchical analysis	Division	The method is tuned for analysis of hierarchy and its impact on risk under particular circumstances.
Systems orientated	Division	The method uses the principles of systems engineering such as decomposition and encapsulation.
Quantitative	Scale	The method uses numerical means to express risk. Typically, methods meeting this criterion tend to be based on probability.
Qualitative	Scale	The method uses classifications as a means to express risk against some predefined scale.
Causal	Event	The method models the causes of an event to assess risk.
Consequence	Event	The method models the consequences of an event to assess risk.
Detailed	<i>None</i>	The method involves a detailed understanding of the system under analysis. Methods of this type will inevitably require a significant amount of data on the system and effort to construct.
Top down	Start	An analysis using a method with this characteristic will begin the analysis of the system from a top event through a series of relationships eventually uncovering the underlying elements that drive an event.
Bottom-up	Start	An analysis using a method with this characteristic will begin with the identification of low-level events which are linked to high-level events eventually culminating in the top-level event of interest.
Anywhere	Start	The analysis may start at any point.
Diagram based	Documented	The method uses a diagram as the principal means to convey relationships between the various components. A typical example is Fault tree analysis.
Descriptive	Documented	The method primarily uses a description of the system as a basis of the analysis

Attribute	Classification	Description
Mixed	Documented	The method uses a mixture of descriptive analysis and diagrams.

Table 13 Risk analysis methods - attributes and qualities

Method	Acronym	Category			Focus			App		Specialist Application	Historic data	Model			Division		Scale		Event		Start			Documented		
		Traditional	Sociotechnical	Other	Technical	Human factors	Organisational	Retrospective	Predictive			Conceptual	Abstract	Instance based	Hierarchical analysis	Systems orientated	Quantitative	Qualitative	Causal	Consequence	Top Down	Bottom Up	Anywhere	Detailed	Descriptive	Diagram based
Swiss Cheese Model	SCM		✓			✓	✓				✓				✓			✓						✓		
Australian Transport Safety Board - Swiss Cheese Model	ATSB-SCM		✓			✓	✓	✓			✓				✓			✓						✓		
Failure Modes and Effects Analysis	FMEA	✓			✓				✓									✓			✓					
System Theoretic Accident Model and Processes	STAMP		✓			✓	✓		✓			✓	✓					✓		✓					✓	
Event Tree Analysis	ETA	✓			✓				✓					✓			✓		✓	✓				✓		
Fault Tree Analysis	FTA	✓			✓				✓					✓			✓		✓	✓				✓		
Hierarchical Task Analysis	HTA			✓		✓				✓				✓			✓		✓	✓				✓		
Bow Tie	N/a			✓	✓				✓					✓			✓		✓	✓					✓	
Functional Resonance Analysis Method	FRAM		✓			✓	✓		✓					✓			✓		✓				✓			

Method	Acronym	Category			Focus			App		Specialist Application	Historic data	Model			Hierarchical analysis	Scale		Event		Start			Documented		
		Traditional	Sociotechnical	Other	Technical	Human factors	Organisational	Retrospective	Predictive			Conceptual	Abstract	Instance based		Quantitative	Qualitative	Causal	Consequence	Top Down	Bottom Up	Anywhere	Detailed	Descriptive	Diagram based
Safety Risk Model (<i>with FTA</i>)	SRM			✓						✓			✓		✓			✓				✓			
Bayesian Networks	N/a			✓	✓								✓	✓	✓		✓			✓			✓		
AcciMap	N/a		✓			✓		✓						✓			✓					✓			
Reliability Block Diagram	RBD	✓			✓				✓				✓		✓		✓			✓			✓		
Cause-consequence table	N/a	✓			✓				✓					✓	✓	✓	✓			✓			✓		

Table 14 has been included to provide the Author’s qualitative assessment of each technique to supplement the detailed assessment of Table 13. It lists the techniques perceived advantages and limitations together with other relevant comments. In addition, the assessment includes categorising whether the technique is widely known in the risk assessment community, used predominantly in academic circles, and has a long history. Finally, it identifies the reference material used for each technique.

Table 14 Risk assessment methods - qualities

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
Swiss Cheese Model	SCM	✓	✓		<ul style="list-style-type: none"> • Concept is easily understood • Focus on latent errors and layers of defence • Defence in depth 	<ul style="list-style-type: none"> • It is not detailed • Technical focus lacking 	<ul style="list-style-type: none"> • The measure of risk is the layers of defence and the number of latent errors • It could arguably be applied to either an accident or a design justification 	(Reason, 1997) (Reason, 2016)
Australian Transport Safety Board - Swiss Cheese Model	ATSB-SCM				<ul style="list-style-type: none"> • Classification of risk and mitigation is separated into 5 levels from technical to organisational 	<ul style="list-style-type: none"> • It is not detailed 	<ul style="list-style-type: none"> • The model was developed primarily to investigate accidents 	(Underwood and Waterson, 2013b)

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
Failure Modes and Effects Analysis	FMEA	✓	✓		<ul style="list-style-type: none"> • Thorough analysis of cause and effects • Each failure is considered in turn which leads to an in-depth analysis 	<ul style="list-style-type: none"> • Single systems /components/ subsystems are analysed separately. • Each failure analysed separately and there is no consideration of multiple component failures. • Each level to be analysed separately and joined through tables • Pseudo quantitative risk 	<ul style="list-style-type: none"> • Adding severity, occurrence and detection along with RPN changes it to FMECA although some writers do not differentiate and continue to call it an FMEA. • The method is centred around creating a priority index to address risks in priority order. • Does not deal with combinations of failure as item that is deemed to have failed. The failed item is considered with all others working perfectly. • It is fundamentally a failure analysis method and requires some manipulation to describe risk 	(Anleitner, 2010) (Aven, 2008) (Lepmets, 2017)

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
System Theoretic Accident Model and Processes	STAMP			✓	<ul style="list-style-type: none"> Multi-system analysis The analysis provides several views (hierarchy, process) 	<ul style="list-style-type: none"> Assumes control is imposed from above in the hierarchy. Documentation in several parts Near absence of technical analysis Relies on safety limits 	<ul style="list-style-type: none"> The method does not predict risk as such, rather the safety constraints that are required to maintain safety. Hierarchy is used as a method of decomposition. There is still an element of likelihood reduction in the processing of hazards, but this is in the background 	(Leveson, 2011) (Fleming and Leveson, 2016)
Event Tree Analysis	ETA	✓	✓		<ul style="list-style-type: none"> Logical associations Maps multiple consequence outcomes 	<ul style="list-style-type: none"> Probability based Focused on a single high-level event 	<ul style="list-style-type: none"> The method is documented as able to be used qualitatively by (Aven, 2008), but this is not the normal mode of use. 	(Aven, 2008) (Rail Safety and Standards Board, 2007)

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
Fault Tree Analysis	FTA	✓	✓		<ul style="list-style-type: none"> Logical associations 	<ul style="list-style-type: none"> Probability based Focused on a single high-level event 	<ul style="list-style-type: none"> The method is documented as able to be used qualitatively by (Aven, 2008), but this is not the normal mode of use. 	(Aven, 2008) (Rail Safety and Standards Board, 2007)
Hierarchical Task Analysis	HTA	✓	✓		<ul style="list-style-type: none"> Breaks down tasks Recognises human ability for correction 	<ul style="list-style-type: none"> Not particularly suited to technical systems analysis 	<ul style="list-style-type: none"> Aimed purely at documenting human factors processes. 	(Whittingham, 2004) (British Standards Institute, 2010)
Bow Tie	N/a		✓		<ul style="list-style-type: none"> Logical associations 	<ul style="list-style-type: none"> Probability based Focused on a single event Often used without any quantitative analysis 	<ul style="list-style-type: none"> There are effectively two versions of this method a description tool, which is a managerial picture of risk and an analysis effectively combining an FTA and ETA 	(Aven, 2008)
Functional Resonance Analysis Method	FRAM			✓	<ul style="list-style-type: none"> Looks how the system normally works Variance is measured as a surrogate for risk 	<ul style="list-style-type: none"> Does not express risk in a traditional way 		(Hollnagel, 2012)

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
Safety Risk Model (<i>with FTA</i>)	SRM	✓			<ul style="list-style-type: none"> Wide range of standard risk figures 	<ul style="list-style-type: none"> Uses prior risk figures – can only analyse what is known The model is based on a rotating window of capturing very low-frequency events. Therefore, a single event could skew the figures. 	<ul style="list-style-type: none"> The problem is tailoring the generic figures from the model to particular situations. Using unconditioned figures will result in an analysis that does not reflect the particular situation 	(Rail Safety and Standards Board, 2014b)
Bayesian Networks	N/a			✓	<ul style="list-style-type: none"> Theoretically possible to analyse very large networks of systems. 	<ul style="list-style-type: none"> Quickly becomes very complicated 	<ul style="list-style-type: none"> Computer modelling is the only realistic method of analysis in a network of any size. 	(Marsh and Bearfield, 2008)

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
AcciMap	N/a			✓	<ul style="list-style-type: none"> Provides an easily understandable diagram of the relationships throughout a hierarchy 	<ul style="list-style-type: none"> Can become complicated 	<ul style="list-style-type: none"> Developed from Rasmussen's Risk Management Framework Although described by some as a retrospective method, it is clear it can be used for predictive scenarios The method does not directly calculate risk levels. 	(Svedung and Rasmussen, 2002)
Reliability Block Diagram	RBD	✓	✓		<ul style="list-style-type: none"> A complementary diagram to an FTA approach. Generally, things are expressed in terms of positive functionality Tools are readily available for analysis, e.g. RAPTOR 	<ul style="list-style-type: none"> Probability focused on a single event 	<ul style="list-style-type: none"> By applying this method, an equivalent of the FTA can be created for an application. 	(Aven, 2008) (Rail Safety and Standards Board, 2007)

Method	Acronym	Use			Qualities		Comments	Source
		Long history	Widely known	Academic use	Advantages	Limitations		
Cause-consequence table	N/a	✓	✓		<ul style="list-style-type: none"> Simple presentation with both the cause and consequence effects in only place 	<ul style="list-style-type: none"> It is a simple table which does not lend itself to complex entries. In this case, has to be backed up by a specific study using other techniques 	<ul style="list-style-type: none"> The method is widely known and aligns neatly with the legislative requirements As a by-product, it provides for parallel path analysis 	(Rail Safety and Standards Board, 2007) (CENELEC, 1999)

4.2.1 Assessment conclusions

There are advantages and limitations of using each of the identified techniques.

Therefore, it would be advantageous to allow as many as possible to be used together in a large system analysis. Furthermore, this leads to the conclusion that there must be a process to combine and aggregate the effects into a singular answer for the system as a whole.

The sociotechnical methods appear to have abandoned the traditional approach of using direct measures for risk. Instead, they focus on deviations from the norm and the imposition of limits. While this is understandable when dealing with human-focused processes, it neglects the role that technology plays in preventing and controlling risk. Indeed, the very presence of technology is sometimes as a result of the inability of humans to control risk as has been documented by Institute of Railway Signalling Engineers (2005) for example, when describing the reason for the development of route interlockings as assisting the signaller to avoid setting conflicting routes.

4.3 Summary

The results reported in this chapter are taken forward and used in Chapter 6 to justify and develop a new risk assessment method.

The industry survey, Section 4.1, has revealed that FMEA and FMECA are the most understood and used risk analysis techniques. The newer sociotechnical techniques such as STAMP and FRAM are unpopular. There is no overall best technique as was shown in Section 4.2, instead each technique has a selection of advantages and disadvantages. Moreover, the type of technique can slant the focus of the risk assessment toward aspects such as human factors or hierarchy.

Therefore, the ability to choose a selection of techniques is important to provide a broad analysis.

4.4 Principal points

The principal points from this chapter are as follows:

- i. An anonymous survey has been carried out with 30 valid respondents
- ii. Survey results indicate FMEA and FMECA are the most understood risk analysis techniques followed by FTA and ETA
- iii. Survey results indicate that STAMP and FRAM are not used
- iv. The understanding of risk assessment techniques and the process is similar across the industry
- v. Parts of the CSM process are not well understood but are used
- vi. Each risk assessment method has different advantages and any new method needs allow for as many as possible.
- vii. Most traditional risk assessment techniques cannot be considered to take a system view of risk assessment.
- viii. Sociotechnical risk assessment techniques take a systems orientated view

5 Review of incident data

This chapter forms part of Chapter 3's developed four-point approach to research evidence gathering. Furthermore, Chapter 3, Section 3.4 described the rationale for the various activities undertaken in this chapter. This chapter contains the evidence from the incident data review from which insights can be drawn. The data also forms a convenient source of material for the cases described in Chapter 7 and Chapter 8.

The RAIB formally gathers data for major incidents on the GB mainline. The resulting analysis is published as a set of publicly available reports. As was described in Chapter 1, over a decade¹² has passed since the last large scale accident, which resulted in a loss of life (Rail Safety and Standards Board, 2017). However, there have still been fatal incidents involving workers. Consequently, despite the headlines, the operation of the railway has not been loss-free over this period as is shown in the data below.

5.1 Incident data

RAIB provides a series of publicly available reports into accidents, entitled 'Accident Report' on their website. The dataset covers both the mainline railway and non-mainline operators. The primary interest of this research is the mainline railway. Given the span of reports, it is important to categorise them into types whereby salient reports can be selected for examination.

¹² Since the time of writing a fatal accident has occurred in Scotland August 2020, due to a landslip.

These reports are of interest as they provide objective evidence about the nature of accidents and incidents that either supports the need for a multisystem risk analysis method or indicates that this is not necessary.

5.1.1 Method

First, the reports were screened to eliminate those that did not refer to the GB mainline railway. Next classifications were drawn from the reports by reviewing the summary of the incident. These were used to identify the part of the railway involved, whether staff or the public were involved and the type of activity being undertaken. Further classification was undertaken to identify those incidents that involved several systems or have a direct environmental factor contributing to the cause as indicators of a possible complex hazardous environment. The analysis treats the environment as a significant additional subsystem. Table 15 explains the classifications:

Table 15 Classification definition

Classification	Description
Train	The incident cause emanated from the train part of the rail system.
Infrastructure	The incident cause emanated from the infrastructure part of the rail system.
Track worker involvement	Track workers were involved in the incident. Usually, this indicates a track worker has been struck by a train, or there has been a near-miss. Often track workers rely on a human lookout for protection
Member of the public injured	A member of the public was involved in the incident. It usually indicates that a person has been struck by a train or there has been a near-miss.
Operational	The incident occurred as a result of an activity that is part of the normal operation of the railway
Maintenance	The incident occurred as a result of maintenance activities
Construction	The incident occurred as a result of a construction/renewal activity.

Human error	The incident was a designated as human error that led to the wrong side failure. For example, crossing the line when it was not clear. These instances could in some cases be due to deeper system problems, as articulated in the New View philosophy of human factors.
Component failure	The incident was due to a component failure
Subsystem failure	The incident was directly due to the failure of a subsystem to function as intended
Multisystem event	Several systems were directly involved in the incident. These could be either technical or human.
Environmental effect	Environmental factors such as a vacuum were a direct cause of the incident

An example entry from the analysis table is illustrated below in Table 17. Appendix B shows the full analysis undertaken by the Author. The headings have been created to group the classifications. These are described in Table 16.

Table 16 Heading definition

Heading	Mutually exclusive	Description
Cause based on	Yes	This indicates the cause of the incident
People affected	No	This indicates the groups of people that were affected by the incident. More than one group could be affected
Source of incident	Yes	This indicates the operational state when the incident occurred.
Type of incident	No	This indicates the type characteristics of the incident. An incident could exhibit more than one characteristic.

Table 17 Sample RAIB GB heavy rail accident report extracts reformulated RAIB data

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
Report 19/2016: Overspeed incident at Queen's Park	<p>The driver manager who was being assessed did not slow the train for the emergency speed restriction as he had misunderstood details of the restriction given in an email.</p> <p>The assessing driver manager's knowledge of the emergency speed restriction was insufficient to notice the driver's error.</p>	Yes	No	No	No	Yes	No	No	Yes	No	No	No	No

5.1.2 Assessment conclusions

The figures in this section have been drawn up from the RAIB data analysis conducted by the Author in Appendix B and summarised in Figure 14. As can be seen from Figure 15, that the majority (60%) of the 35 incidents investigated by RAIB between 2016 and 2019 are operational indicating that the highest risk is generally when an asset is in use. Furthermore, the operational phase of an asset represents the majority of the lifecycle; it also accounts for the maintenance of the asset. Consequently, if a risk analysis can effectively predict and address operational and maintenance risks, there is scope to affect 86% of the total incidents positively. Predicting operational risk is an aim of safety risk analysis, and improvement is, therefore, worth pursuing.

It is also worth noting from Figure 16 that there have been 16 incidents that have involved either a multisystem or environmental cause, which indicates that there is a need for an analysis method that provides a whole system assessment of the risk. Furthermore, there are ten indications of a subsystem failure where the components have not failed, but the subsystem has failed to carry out the intended function. Again, this indicates that there is a need to review risk from an overall system risk perspective.

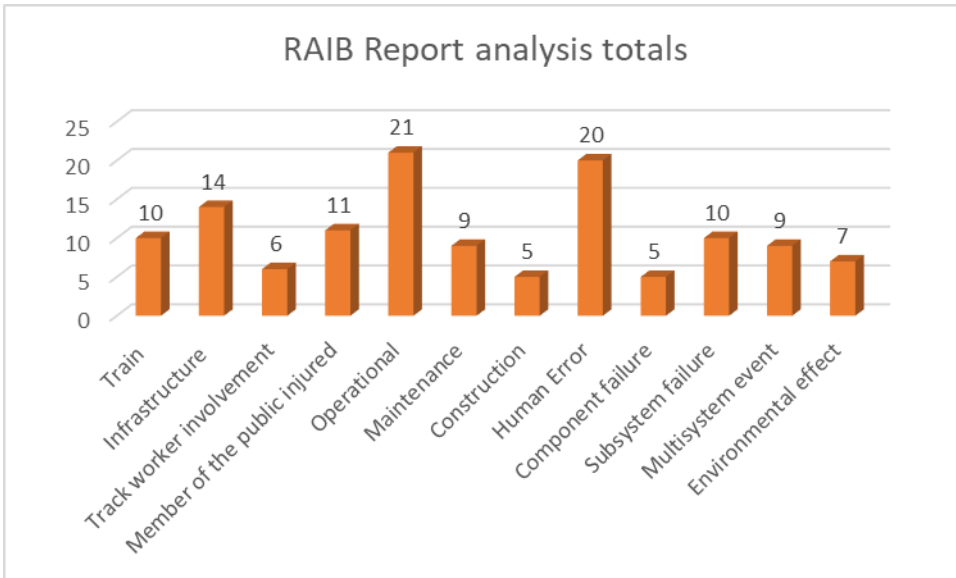


Figure 14 RAIB incident reports -raw category totals

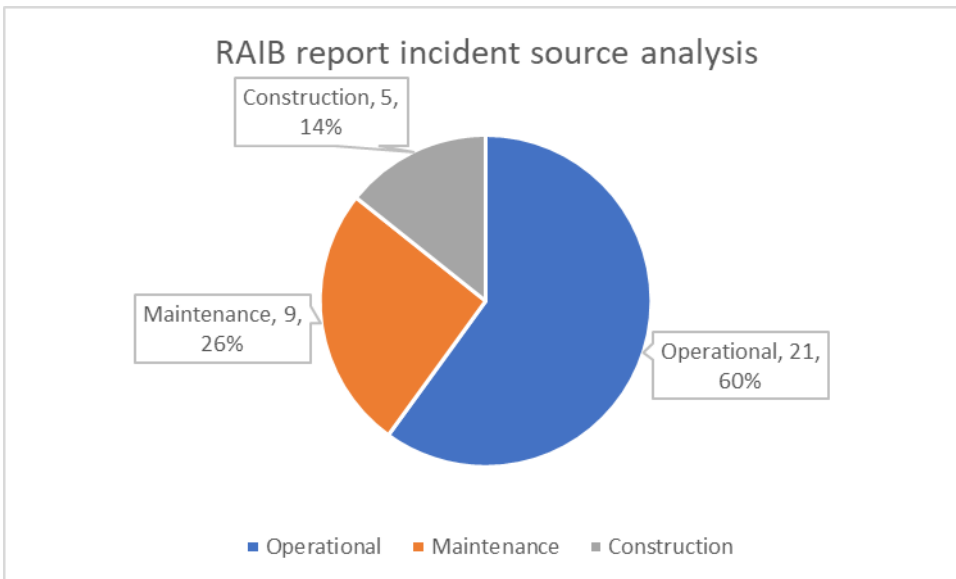


Figure 15 RAIB reports - incident source analysis

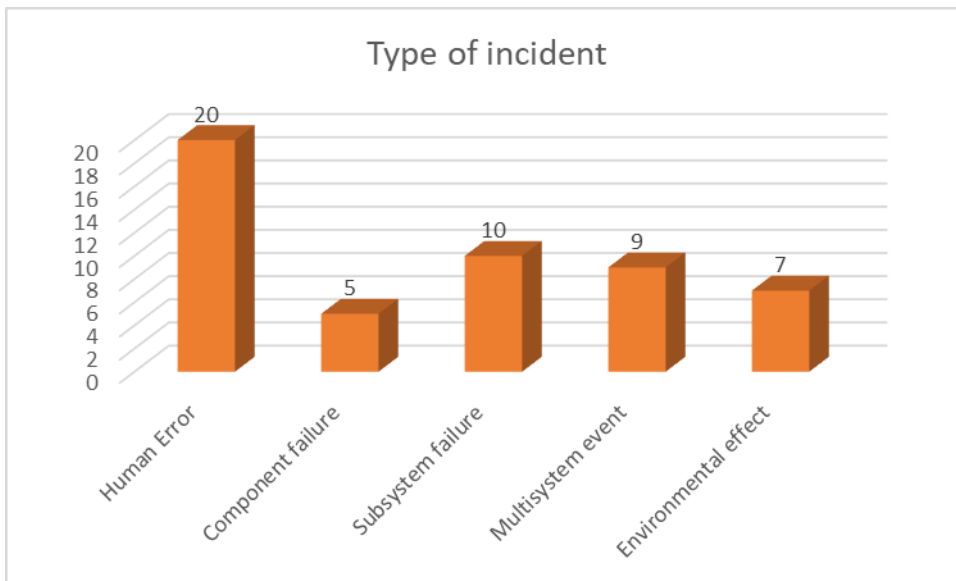


Figure 16 RAIB reports – the type of incident analysis

As indicated by Figure 16, there are 20 human error incidents, further inspection of the analysis in Appendix B indicates that the majority (70%) of these occur when the human is not supported by a physical safety system highlighting the key role technology plays in the prevention of accidents. Therefore, it is also relevant that the risk analysis system provides support for the technological system as well as a method of indicating the risks posed by unsupported humans. In addition, there are a significant number of component failures (14%) at the root of these incidents, which points to the need to maintain a focus on the technological integrity of the risk analysis contrary to the current vogue, as indicated by Hollnagel (2012) for example, to assume that components are totally reliable. Consequently, any proposed system must still address the technical risk as well as others caused by the integration of systems and humans into socio-technological systems.

5.2 Summary

The RAIB data has been subject to an analysis described in this chapter which illustrates the complex nature of railway incidents. It has shown that a significant

number of incidents have been multisystem in nature and technological failure is still occurring. This data is taken forward and used in Chapter 6 as evidence in the justification for a new method.

5.3 Principal points

The principal points from this chapter are as follows:

- i. 70% of human error incidents occur when not supported by a physical safety system
- ii. 45% were multi system incidents
- iii. A significant number of failures (15%) had component failures at the root of the incident

6 Composite Assessment Method (CAM) – new model and method

The purpose of the new method, the **Composite Assessment Method (CAM)**, is to fully analyse complex or multi part systems for safety risks and their criticality.

This analysis will enable legal requirements to be fully satisfied in addition to the moral and commercial imperative of reducing risks.

CAM is a causation type of safety risk assessment method; it can be used to understand safety risks for the whole system or at nominated points in a system. A holistic or partial analysis can be undertaken to assess safety risk, but for a partial analysis the result will only reflect the risks of the components included in the analysis.

The objective of this chapter is to define and describe CAM. First, a rationale for CAM is provided, followed a short description of candidate current techniques and then by a description of the CAM method. Finally, a demonstration application is included.

As described in Chapter 1 Section 1.9, chapters 2 to 5 have been used to gather information about risk assessment methods and the nature of safety incidents on the railway. This information is used in this chapter to create and justify CAM.

6.1 Rationale

Chapter 2 appraised the current methods, primarily dividing techniques between new methods of the sociotechnical type, such as STAMP, and those ‘traditional’ methods that have been in existence for decades, such as FMEA and FTA. The industry survey (Chapter 4) reported that traditional methods, like FMEA are

familiar to practitioners. Inclusion of these methods as part of CAM reduces the training requirement for its use. STAMP, on-the-other-hand, was shown in Chapter 4 to be unpopular and reported by Underwood and Waterson (2013b) to be complicated. Chapter 4 indicates similar findings for other sociotechnical methods such as FRAM. Therefore, by using traditional analysis methods in the CAM process, some of the barriers to use will be overcome.

A review of RAIB incident data was undertaken in Chapter 5. It found that 45% of incidents involved multiple systems, and 14% of the incidents included component failures as a cause, moreover, 70% cited human error as a contributory factor. Therefore, CAM should cater for all these features, including the analysis of multiple systems.

Chapter 4 survey results indicate that some risk analysis is performed during integration of the system, it also shows that the sociotechnical methods are unpopular. This implies that 'traditional' risk analysis methods are used during the integration risk analysis. Some of the 'traditional' methods could be adapted to provide an 'overview'. However, this risks a superficial analysis, analogous to reducing the magnification on a microscope. Consequently, critical hazards could be missed allowing systems with latent risks to be given a 'clean bill of health'. While the reverse is also true for a complex system, (INCOSE, 2015) and (Leveson, 2011) among others point out that hazards that emerge at the systems level are not visible at the subsystem level and hence could be missed if not accounted for at the system level.

Chapter 2, described that authors such as Leveson (2011) argue that the 'traditional' methods were developed before isolated systems were interconnected

and they were optimised for an isolated system environment. They argue that they are not suitable for an interconnected environment. The advantages of systems analysis techniques for the analysis of complex systems were also reviewed, and it is evident that the systems approach is an advantage in a complex or multi part system scenario.

The review in Chapter 2 indicated that models such as Bayesian Networks quickly go beyond human understanding due to the matrix of Joint Probability Tables at each vertex. Marsh and Bearfield (2008) acknowledge this complexity. It is an example of Manson's (2001) algorithm complexity. Consequently, it leaves the analyst without a good understanding of why the analysis has produced the result. It may well be possible to create computerised tools to hide the complexity. Sanford and Moosa (2012) acknowledged the difficulty of creating such a tool and declared Bayesian Networks analysis as a Non-deterministic Polynomial-time Hard (NP-Hard) computing problem.

The Author is of the opinion that understanding the analysis is an essential component of producing a good analysis. Expert opinion plays a large part in predicting future risk when undertaking a risk analysis. This opinion is influenced by belief (Shafer, 1976), where the actual numbers do not necessarily strictly follow the laws of probability. Purely probabilistic models such as Bayesian Networks may suffer as a result of this effect.

The review of the current risk analysis methods undertaken in Chapter 4, Section 4.2, concluded while there is no overall best risk assessment technique each method has positive and negative features that can slant an analysis towards a particular type of risk identification. For example, STAMP (Leveson, 2011) focuses

on the fallibilities of management and process systems. Therefore, it is important that as wide a selection of techniques be available as possible in the subsystem analysis part of CAM to provide the analyst with flexibility.

Sociotechnical methods focus on the fallibilities of management and process systems, for example FRAM (Hollnagel, 2012) and STAMP (Leveson, 2011), claim to take a system engineering approach. The physical system is almost forgotten in the creation of safety limits with these later methods. This paradigm is contrary to the physical world, where the physical item is becoming ever more critical and complex, for example the Eurofighter (Posey, 2012).

CAM is a potential improvement over current techniques because it combines the advantages of a systems approach to safety analysis with the use of 'traditional' methods in parts of the process.

Through a combination of systems and traditional techniques, CAM makes it possible to carry out a full system in-depth analysis and avoid many of the complications associated with newer methods like STAMP by allowing the analysis of each subsystem in isolation. Furthermore, the isolated subsystem analyses, reduces the complexity of the whole analysis and keeping it to an understandable level for the analyst; this aligns with the complexity concepts of Manson (2001). Finally, these parts are brought together again using system engineering methods in a rule based way to provide the results for the full analysis.

It is concluded that the current methods leave a gap to be filled by CAM.

6.2 Candidates for CAM

Several candidate techniques were considered for repurposing as CAM:

- Bayesian networks,
- Functional Resonance Analysis Method (FRAM),
- Swiss Cheese Model (SCM),

Bayesian networks (Marsh and Bearfield, 2008), have been shown in Chapter 2 to suffer from computational difficulty, which does not meet the objective of simplicity and understandability. FRAM (Hollnagel, 2012), incorporates the concept of links that may or may not be present. However, it does not use risk as such, and fundamentally it detects variation. Furthermore, FRAM does not allow for other models to be incorporated into the method. Consequently, it fails the test of allowing the use of familiar techniques such as FMEA. SCM, originally described by Reason (1997) and updated (Reason, 2016), provides a simple conceptual model. A practical version, as used by the Australian Transport Safety Board, is described by Underwood and Waterson (2013b). This model appears to suffer from concentrating on the hierarchy of risk rather than the actual risk and is, as Reason reiterated (Reason, Hollnagel and Paries, 2006), a much better conceptual framework than a detailed risk analysis tool. Parts of the model have been criticised as not being tightly specified, for example the “holes”. In many ways this is a strength because it is a visual concept, but it is also a weakness because interpretations can differ. The Australian Transport Safety Board version of the model has some more detail but essentially relies on setting out a question framework to be answered by the analyst against conceptual levels that are designated as “safety factors” and “safety issues”; the remainder of the process is

left to the analyst to resolve, as described by Underwood and Waterson (2013b). This is probably adequate for the application of a specific accident investigation but leaves many questions unanswered for general applicability.

All of these options were rejected in favour of the method explained below.

6.3 Method

Firstly, CAM is explained as an abstract concept, followed by an architectural description, and finally the details are explained. Initially, some terms are mentioned without a full explanation, these follow later.

The term system is a label for an overall object that performs a set of functions.

The term subsystem is a part of a system that can be regarded as a system in its own right. The term component is used to refer a part of a subsystem or system.

This thesis attempts to follow this convention. Occasionally, the labels systems and subsystems are used interchangeably because their use depends on the viewpoint of the observer with respect to other objects. CAM can accommodate combinations of systems or subsystems that are connected together. Therefore, from a CAM analysis perspective, it does not materially matter what label the objects have; they are simply a group of objects to be assessed within an overall scheme.

6.3.1 Success for CAM

CAM is to be useable by practitioners in the field. Usability is a key finding from a survey Underwood and Waterson (2013a) where 54% of respondents identified ease of use as a determinate of the usefulness of a technique. Therefore, for the most part, complicated mathematical formulae are avoided; instead, concepts and simple associations guide the construction of the method. Furthermore, there is an

emphasis on borrowing parts from existing techniques and recombining them in novel ways to produce a scheme with links to understood techniques.

CAM should be generally applicable and should sit separately from any particular context. The analysis sets out to address systems defined by EN15288 (International Standardization Organization, 2015, p. 9) as a “combination of interacting elements organized to achieve one or more stated purposes”. This definition includes physical equipment, people and processes. Data is considered an attribute of a system, used to influence system behaviour and to be passed between systems.

The output of CAM should be compliant with the current legal requirements for risk assessments. It is an essential requirement, as was discussed in Chapter 2, and is a noted fault of STAMP (Dunsford and Chatzimichailidou, 2020).

6.3.2 Concept for CAM

At an abstract level, in concept, a CAM analysis is analogous to a Lego model construction where the objective is to build a model; for example, an aeroplane, by building the wings and body separately then bringing them together to create the full model. In this process, first the appropriate bricks are identified for the model construction. Next, individual subparts are constructed using the bricks, and then subparts are (combined) stuck together using the interfacing bricks to create the overall model.

Similarly, for the CAM risk analysis, the subsystems are identified through diagrams first. Next, subsystem risk assessments are carried out. These are brought together by integrating the analyses into a single view through a CAM specific combinatorial method. This single view contains all the detected safety

risks within the system. The result can be simplified to remove risks that do not affect the overall system. However, from systems theory (INCOSE, 2015), further risks could emerge due to the integration of the parts. Therefore, iterate to re-examine the overall system to check for additional safety risks emerging due to the integration, by reviewing the previous steps and incorporating any changes. Finally, the results are summarised and focused on critical safety risks. Figure 17 illustrates these main conceptual components of CAM.

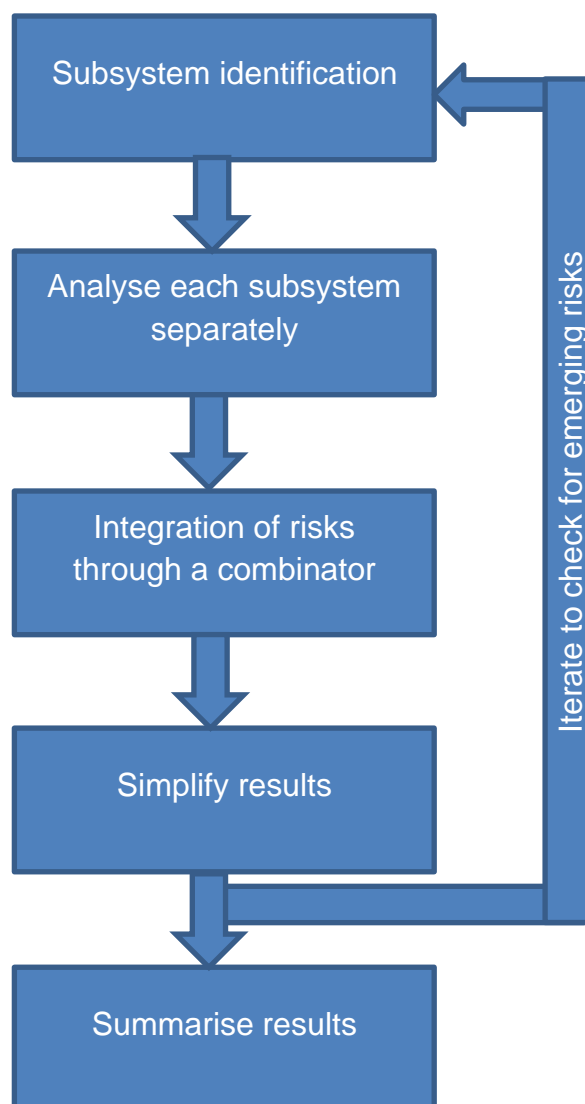


Figure 17 Simple conceptual diagram of CAM

6.3.3 Architecture of CAM

CAM uses the systems engineering concept (INCOSE, 2015) and the systems standard EN15288 (International Standardization Organization, 2015) that systems have internal (compartmentalised) workings, but externally only those things at the interface can be seen and are essential for an analysis. These interfaces are both internal between subsystems and external to the world beyond. The interfaces contain the safety risks that are of interest in a CAM analysis¹³. Figure 18 depicts this concept.

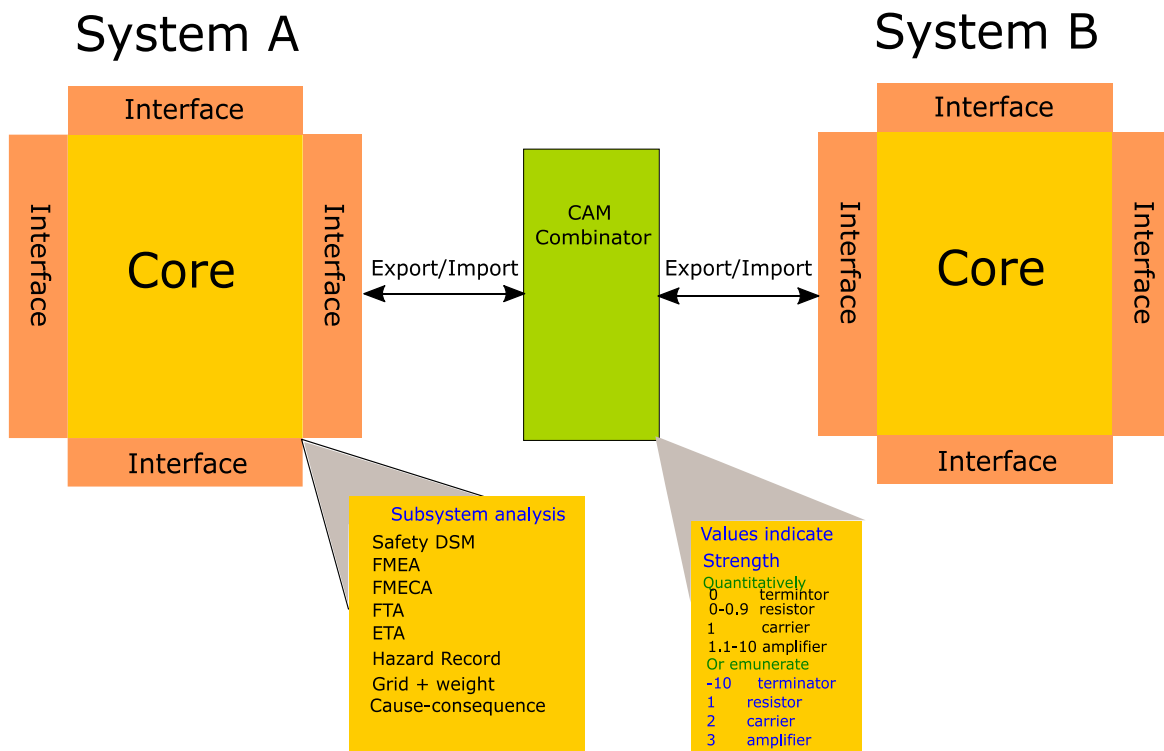


Figure 18 CAM system conceptual overview

When systems or subsystems are interconnected via the interfaces, their effect on each other will be one of four things. It could amplify the risk, carry it over to the next system unaltered, reduce it in the next system, or prevent it from going

¹³ Complete subsystem failures can be represented in this model by risks at the interface.

further. The CAM Combinator (CAM-C) example, shown in Figure 18, is used to signify there is a link between two systems and the type of effect the link represents. The type of link will be one of the four effects. In a practical system, there are many links between the various subsystems.

By using the building blocks, referred to earlier, of individual subsystem analysis and the CAM-C, in the same way as the Lego analogy, a risk model can be constructed for the whole system. These building blocks can be put together in a variety of combinations to model any overall system.

However, in practice the analysis for a large system could be carried out by a number of parties who may use different scaling of risk variables or different techniques. Simply joining two sets of analyses together is likely to result in a distorted overall analysis. Scaling and translation will enable a uniform set of data to percolate between systems, as shown in Figure 19.

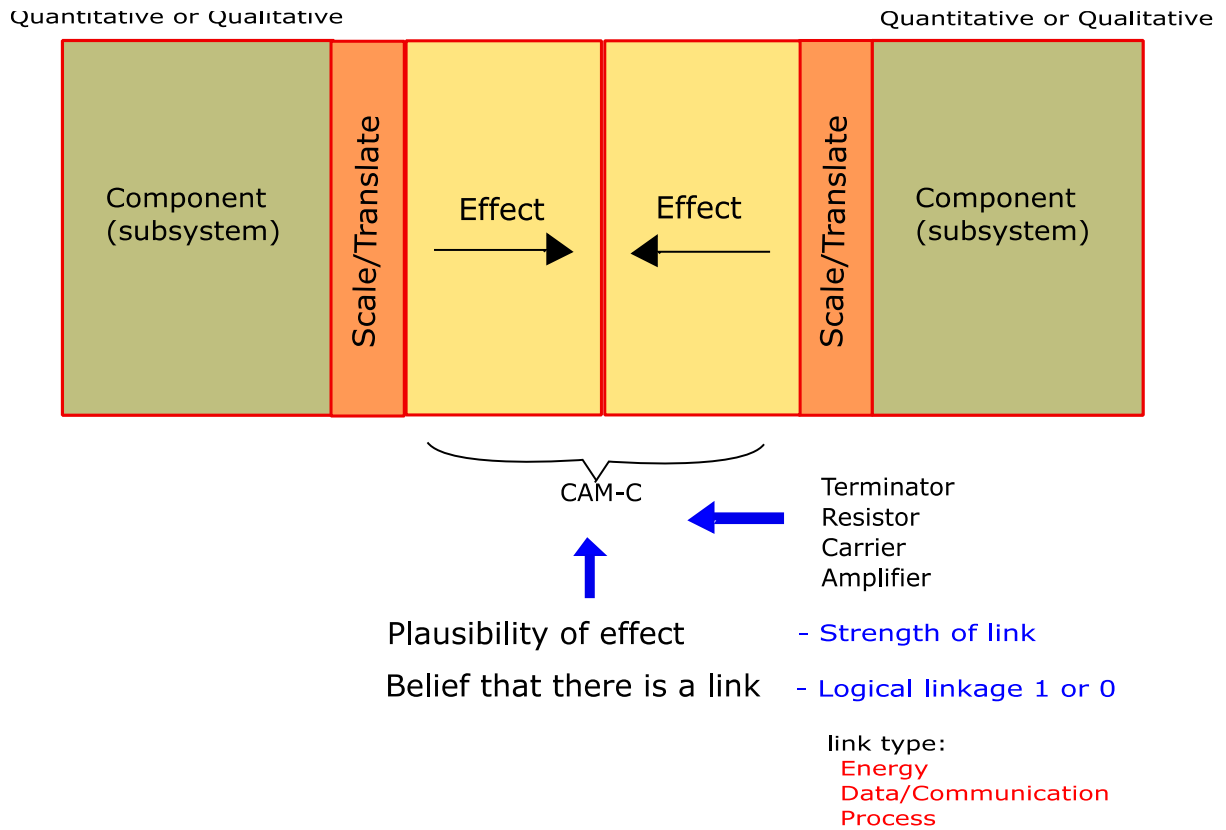


Figure 19 Detailed conceptual diagram of method CAM-C

This scaling and translation subprocess enables a CAM analysis to be successfully carried out for the whole system, even if the subsystem analyses have been performed by different organisations.

6.3.4 Process description of CAM

Further details of the concepts and architecture are given in this section. Stages of the process are listed followed by a detailed explanation in the subsequent paragraphs.

The list below recasts the conceptual five blocks, shown in Figure 17, into process stages with technical labels:

1. System definition
2. Subsystem analysis

3. Integrate the analyses
4. Rationalisation
5. Summarise the output

Stages one to four are iterated until no further risks emerge due to integration, as described in Section 6.3.4.5.

The following paragraphs summarise each of the five CAM process stages.

6.3.4.1 Stage 1 - system definition

As indicated earlier in this chapter, CAM analysis incorporates a system engineering approach. As pointed out by Underwood and Waterson (2013b), systems engineering requires limits to be placed on the analysis, together with an understanding of what the system consists of and its boundaries. This is also a legal requirement of CSM-REA (2013).

The first stage is to create a pictorial diagram of the subsystems that comprise the overall system. The method uses a tool called the CAM Entity Relationship Diagram (CAM-ERD). This diagram is adapted from similar diagrams by Rasmussen (1997); Figure 20 shows a simple example. In the case of CAM-ERD, directed graphs indicate the flow, principally hazard/risk¹⁴, between subsystems. It also includes a triangle to signify the point or points of harm to help focus the subsequent analysis.

¹⁴ Risk is used but other notes could be added to help understand the system relationships.

Figure 21 shows a CAM-ERD equivalent to Figure 20. As can be seen, there is more detail in the CAM-ERD version which helps with the later stages of the analysis. Example risks are attached to the arrows, such as 'unstable'.

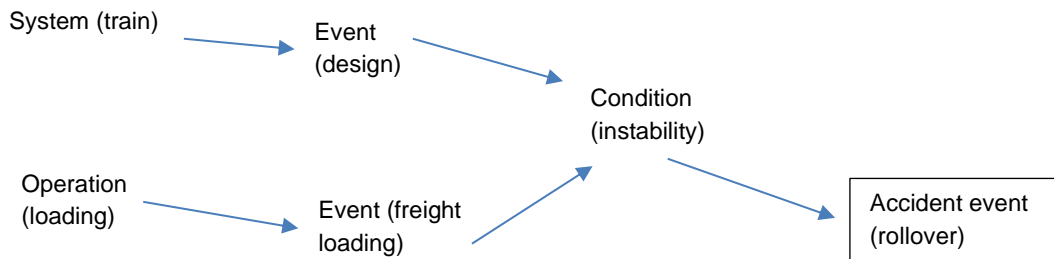


Figure 20 Accident diagram in the style of (Rasmussen, 1997)

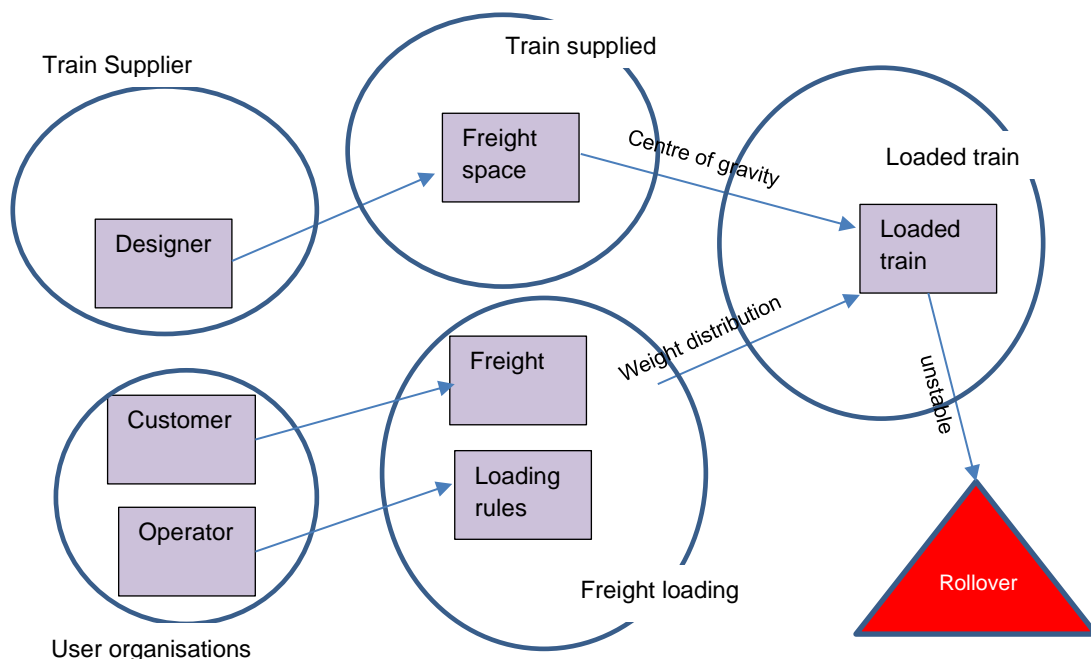


Figure 21 CAM-ERD

As can be seen in Figure 21, circles are used to group parts (shown as rectangles) into nominal subsystems to aid the next stage of the analysis. The CAM-ERD diagrams are constructed from documentation on the system. Brainstorming or HazOp techniques can be used as an aid to identify the hazards/risks and parts of the system.

6.3.4.2 Stage 2 – subsystem analysis

The second stage of the CAM process is to analyse the subsystems using a method of the analyst's choice.

Chapters 2 and 4 show that the 'traditional' methods are suited to this type of isolated analysis. Leveson (2011) among others has indicated these methods were developed in an era of isolated systems and are suited to an isolated subsystems analysis. Chapter 2 has also indicated, contrary to Leveson (2011), that these techniques do not rely on sequential chains and are again suited to the modern subsystems.

The output of these subsystem analyses is used in the CAM process to produce a more complete answer and feed into stage 3.

It may be an advantage to use existing assessment data as an input to this stage of the process and reduce the effort required.

Some methods are easier to use with CAM than others. Section 6.3.8 contains a list indicating how straightforward each is to use. The flexibility on the choice of method gives rise to a potential danger that the risk data cannot be integrated in the later stages of CAM. This danger arises because not all methods use the same internal properties. However, CAM has been designed to cope with this danger and can handle various types of data produced by the subsystem analysis methods. CAM includes a subprocess, mentioned in Section 6.3.3 to convert data to the required risk-based form at the end of the process. An example is the use of the popular FMEA and FMECA techniques which handle failure data.

Fundamentally not every failure is a safety event as was observed by Lepmets (2017); therefore, there will be a difference in the frequency between failures and

those same failures causing a safety event. In the case of an FMEA the conversion in CAM is achieved by adjusting the frequency.

6.3.4.3 Stage 3 – integrate the analyses

The third stage of the CAM process is to integrate the risks identified through the individual subsystem risk assessments in stage 2 through a combinator.

Chapter 2 highlighted methods from systems engineering described by Eppinger and Browning (2012) with the Domain Mapping Matrix (DMM), partially identified by Bonzo, McLain and Avent (2016), the most promising. An analysis was carried out by the Author in and it was found that the Multi-Domain-Matrix (MDM) was superior for use in CAM because it is possible to combine several DMMs into a single table. Furthermore, cell values were influenced by the works of De Lessio, et al. (2015) and Parmar and Lees (1987). The Author asserts the resulting combination together with the application of MDMs in safety analysis is novel, and is described below as CAM-C.

The combinator, CAM-C, is the key to the operation of CAM. As was outlined in Section 6.3.3, it is a method of mapping how risks at interfaces link together through a matrix. All the subsystems are combined in a single step into a single large CAM-C. This combinator is adapted from the MDM developed by Eppinger and Browning (2012). The matrix is a pairwise link descriptor matrix, similar to a spreadsheet; the matrix columns are inputs, and the rows are outputs. A figure in an intersecting cell indicates that a link exists. The value of the figures put into the intersecting cells describes the type of link. To populate the CAM-C, if there is a risk from a lower level subsystem causing a risk in the high-level system, insert a figure in the intersecting cell. Figure 22 shows a CAM-C extract example; the data

has been extracted from an analysis carried out by the Author using CAM. Each risk is given a reference number: 103 represents the risk of 'path too steep', while 104 represents the risk of 'material washed away'. In this case the numbers in the intersecting cells represent 'carrier' links which are described later in this section. For example, risk 103 is an input causal risk for risk 104 in Figure 22.

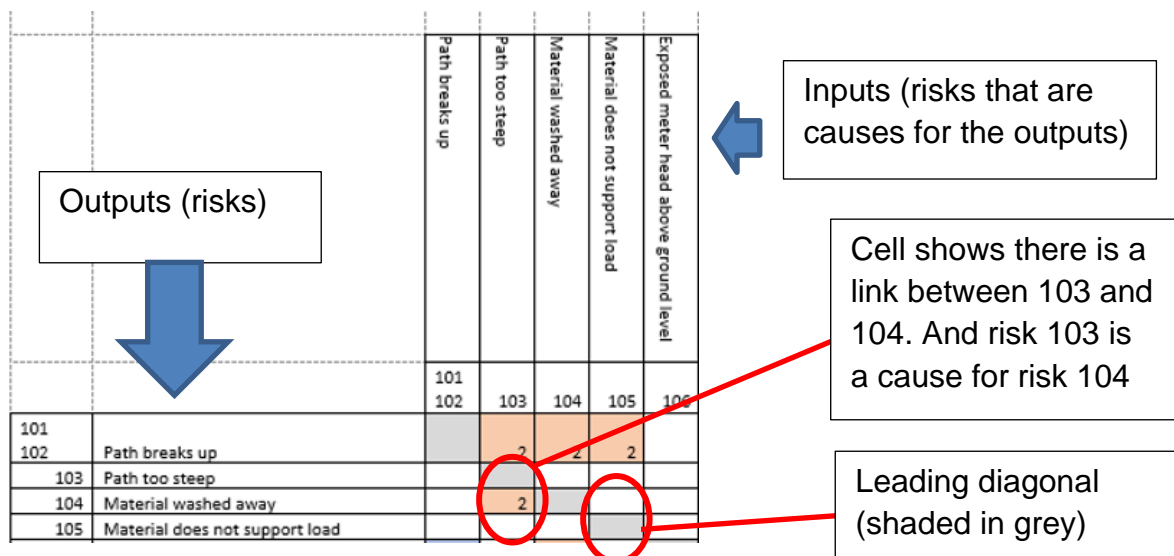


Figure 22 An example extracted from a CAM-C

Logically it is possible to describe the higher-level risk by the aggregate of the risks acting as causal risks. Therefore, with some exceptions explained later, the entries along a row in a CAM-C indicate the lower-level causal risks that describe the higher-level output risk on that row.

Individual risks identified in stages 1 and 2, are traced from the overall system through CAM-C matrix to the source in the subsystems. This tracing is an iterative process through the subsystem and part(s) levels. Figure 23 illustrates tracing using an extract from an analysis carried out but the Author. It shows a number of major subsystems, these are colour coded and have references assigned in ranges of 100. The meaning of the risks is unimportant for the illustration.

			Culvert		Pipes	Ballast		Sleepers		Drain	
			101 102	103	104	105	201	202	203	204	205
Culvert											
	101 102	Blocked									
	103	Structural collapse									
	104	Water leaks out of manholes				3					
Pipes											
	105	Flow not enough									
Ballast											
	201	Fallen away									
	202	Washed away									1
Sleepers											
	203	Moved		2							
	204	Sleeper not supported					3	3		AND	
Drainage											
	205	Overwhelmed			2						

Figure 23 Multi-subsystem CAM-C tracing illustration example

The analyst looks along the row of an overall-system risk and identifies the inputs; this is where a figure corresponds to a column. In this case 205 has a “2” in risk 104 column. The column is a risk, which is a causal risk contributing to the higher-level risk. This causal risk is then used as the next risk row to be traced. In this case risk 104. The process identifies causal risk iteratively until the path (trace sequence) terminates. In this case 105, the pipe risk of ‘flow not enough’ is the

root causal risk. This process can also be operated in reverse to trace from root causal risks to system level risks.

CAM-C can be used to remove intermediate and system-level risks from the analysis and identify the root causes through the trace. This action is logically valid only when the aggregate of the causal risks on the row describes the risk entirely. Where this is not the case that risk row must be retained, because there is some unique quality extra to the causes and the risk is designated as 'partially described'. This property is signified in CAM-C by placing a partially described (PD) label on the leading diagonal, an example is shown as part of the demonstration in Section 6.6.4.

The cause tracing through CAM-C implies for each row that the individual causal risks are related to the output risk by a logical OR relationship; where each causal risk contributes a portion of the total output risk. Furthermore, the iterative link from column to a row, described in the previous three paragraphs, implies a logical AND relationship in a chain, albeit a simplified one. However, some risks only materialise when several causes on that row occur at the same time. The individual causal risks are in this case related through a logical AND relationship. CAM also provides for this type of AND relationship in the model. The analyst inserts a special row to indicate that it must be handled slightly differently in the assessment. The effect is to reduce the likelihood of the risk's occurrence by assigning the lowest frequency of the causal risks to the output. This type of row is denoted by 'AND' label on the leading diagonal. Figure 23 gives an illustration of the AND relationship for risk 204, it is dependent on the causal risks 201 and 202; both have to occur for risk 204 to be realised.

CAM-C can operate in two modes, either as a qualitative or quantitative model. If a quantitative analysis is undertaken, the numbers reflect the scaling of the risk between the subsystems. If a qualitative model is used, the figures used are enumerators for the types of link previously described. A table of suggested values is shown in Table 18 below.

Table 18 CAM-C values

Link-type	Mode	
	Qualitative	Quantitative
	Cell enumerator	Cell scalar
No link	Blank	Blank
Amplifier	3	$x > 1$
Carrier	2	$x = 1$
Resistor	1	$0 < x < 1$
Terminator	-10	$X = 0$

Where x is the cell scalar value.

An entry in a CAM-C cell from Table 18 provides a mechanism to express three qualities, the belief that a link exists, from Shafer (1976), the plausibility of the link and the type of link. The four types of link and their effects were mentioned in Section 6.3.3; a more detailed explanation is provided here. A terminator link, in most scenarios, will represent a link where the effect of the risk will not noticeably materialise in the following subsystem or system. This type of effect is described by Hollnagel (2012) in FRAM as ‘system noise’. The amplifier can be thought of as analogous to Hollnagel (2012) property of ‘resonance’. The effect of the risk will be increased in the following subsystem. Not all reductive links will be of an amplitude sufficient to act as a terminator, instead, some will attenuate the effect to a degree, effectively absorbing part of the risk on the following element, and can be thought

of as a resistor. The function of a carrier link is to transmit the risk unaltered to the following subsystem.

6.3.4.4 Stage 4 – rationalisation

Rationalisation of the analysis results is part of the fourth stage. CAM-C is manipulated to rationalise the risk analysis. The methods used are summarised below:

- Remove intermediate risk
- Remove internal risks
- Remove risks that rely on terminator links
- Remove duplicate risks
- Limit the analysis detail to a level that is useful

Each is described in the following paragraphs.

In this section reference is made to removing values from CAM-C cells. In practice to facilitate future auditing it is better to colour code the cells and conceptually remove the cell from the analysis.

As has been described in the previous paragraphs explaining Figure 23 in Section 6.3.4.3, it is possible to eliminate intermediate risks through cause tracing and replace the overall risk with a series of root cause causal risks. These root cause causal risks are suitably scaled using the aggregate CAM-C link values to scale them to reflect their effect at the system level. The intermediate risks can then be removed from further consideration in the analysis.

A further rationalisation is possible through three mechanisms. These are based on two premises: for a subsystem risk to affect the overall system, it must to interface to it. Furthermore, the subsystem risk has to be able to transmit the risk through intervening subsystems to the overall system. The first rationalisation mechanism¹⁵ is to eliminate those risks that only feed causes within a single subsystem because they will not influence the overall system. Second, is to eliminate those causal risks that link to a risk by terminator links because these are prevented from influencing the overall system. Third, eliminate any duplicate causal risks because they have already been accounted for in the risk analysis. These eliminated elements do not need to be considered further in the analysis. An example is given in Figure 24.

		Path breaks up	Path too steep	Material washed away	Material does not support load	Exposed meter head above ground level	Structural failure	No friction	Loss of grip	Loss of grip and bike skids away	Fall off	Fail to stop
		101 102	103	104	105	106	201	202 203	204 206	205	301	302
101	Path breaks up											
102	Path breaks up		2	2	2							
103	Path too steep											
104	Material washed away		2									
105	Material does not support load											
106	Exposed meter head above ground level	3		3								
201	Structural failure											
202	No friction											
203	No friction											
204	Loss of grip											
206	Loss of grip											
205	Loss of grip and bike skids away											
301	Fall off	2		2	2	3	-10		2			
302	Fail to stop											PD

Figure 24 CAM-C example extract

Figure 24 shows some risks associated with subsystems. It uses number ranges of 100 to differentiate between subsystems. So, risks 101-106 belong to one

¹⁵ Internal linkages enable the analyst to understand how risks propagate through a subsystem, especially where it is complex. Under these circumstances it may not be clear at first sight that an input risk is related to another input risk with an output. Where there is a serial linkage between an input and output through a series of internal links care must be taken to ensure this input-output relationship is not lost in the rationalisation. The analyst should perform a mini rationalisation for the subsystem to relate the inputs to outputs and amend the CAM-C accordingly.

subsystem, and 201-206 belong to another. The links coloured in orange all link within a single subsystem and therefore are not exported to any other subsystems. Removing the numbers from the matrix eliminates the links. Causal risk 201 is linked to risk 301 through a terminator link. This risk link can be similarly removed from the matrix. Removing the numbers from the CAM-C cells¹⁶ effectively eliminates the causal risks links from further consideration in the analysis.

Finally, risks can be traced through to their root causes by following the tracing method described above. However, it may be more appropriate to curtail trace and summarise the causes after a particular number of subsystem links have been traversed. It can be the case, for example, that the analyst cannot influence the safety of components beyond a certain level of decomposition through rework. For example, where off the shelf equipment had been purchased and used with say a Windows operating system, Microsoft will not change the operating system no matter what the analyst says. It will be for the analyst and the engineer to reconfigure other parts of the system to compensate for any risks arising from the operating system and indicate there is a risk with the operating system in the analysis, but it is of no help to pursue details of which line of code is at fault. Under these circumstances, it would make sense not to pursue the risk analysis beyond this point of influence. Instead, it is better to recognise the risk at a level where it can be influenced and deal with it.

6.3.4.5 Iteration

Chapter 2 identifies that in systems theory (INCOSE, 2015), there is a potential emergent behaviour, or in this case, risks, that are observable in the overall

¹⁶ In practice it is better to colour code the cells just in case mistakes have been made during rationalisation.

system. These risks would not be detectable at the subsystem level. CAM uses iteration to check for these risks by requiring the analyst to review the analysis for any emergent risks and incorporate these into the analysis. This iteration process is carried out by analyst repeating stages 1 to 4 and adjusting the analysis as appropriate if the emergent risks when inserted into the analysis make any significant difference to the analysis output.

6.3.4.6 Stage 5 – Summarise the output

As a penultimate step, each of the salient risks are placed into a cause-consequence table to conform to the CSM legislation, (CSM-REA, 2013), as a statement of risk. The table also incorporates the legal requirement to identify the type of evaluation that has been applied. Table 19 shows an example.

Table 19 Cause-consequence table extract example

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Consequence	Control	Evaluation type	Likelihood	Consequence	Risk
104	Manhole leak	High Water flow	Pipes	Pipes do not allow enough flow causing pressure rise and water to burst out of manhole covers and flows at a high rate	Water flows onto the railway	Railway track bed is flooded, and water is fast flowing washing out ballast causing a derailment as injuries	Injuries and possible fatalities	Design control of flow and pressure	Risk Estimation	Occasional	Catastrophic	Intolerable
202	Ballast removal	Track unstable	Ballast washed away	The ballast is not fixed and is washed away by a flow of water	The track is unsupported and becomes unstable. It is unable to support a train	Track moves and derails a train causing injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable

The values in the likelihood and consequence columns are adjusted as described in Section 6.3.5. to document the causal risk effect at the system level.

Finally, a risk matrix similar to the matrix (CENELEC, 2017) presents the results of the analysis. This coloured matrix provides an easily interpretable picture of the acceptability of the risk profile. Table 20 shows an example extracted from an analysis. The red areas indicate where risks are unacceptable, while the yellow areas represent areas where the risk is tolerable.

Table 20 Example risk matrix extract

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					
Probable					
Occasional					104, 408
Rare					202, 203, 204, 205, 401, 402, 406,
Improbable					405
Highly Improbable					301

6.3.5 CAM Heuristic for enumerated ‘amplification’ or ‘resistance’

Section 6.3.4.3 described that a CAM analysis could use a qualitative or quantitative model. When a qualitative model is used the enumerated values have to be translated to adjust the risk likelihood (frequency) and consequence values. A heuristic developed by the Author for the adjustment and it is described in the following paragraphs.

For an amplifier the frequency is doubled. Likewise, the frequency halved in the case of a resistor. Frequency adjustment is the default method, and altering the consequence is done where this can be justified. There is no scientific basis for this, and any factor would be equally as valid. The Author asserts this is valid because the objective is to highlight the key risks and not necessarily to place an exact value on them, in effect applying the Shafer (1976) theory. All risk estimates are matters of judgement, and it is not out of step with standards, where EN50126 (CENELEC, 1999) cites the requirement of the railway authority to calibrate the risk matrix, but then gives no clarity of how to go about it. It appears to point to the

fundamental point that risk is a matter of judgement of physical factors and societal acceptance. The same is true of the updated EN50126 (CENELEC, 2017), there are scaling examples but again no definite guidance on acceptable values.

Where other amplification factors are considered, it should be born in mind that the effect of amplification should be detectable in the analysis otherwise the concept of the criticality of low-level hazards affecting the overall system will be dissipated.

The separation of the causal subsystem from the point of a hazard and potential accident needs to be considered. The influence of a separated amplifier link is likely to be partially dissipated by the intervening subsystems. It will be a matter of common sense for the analyst to judge if the effect at the input has been dissipated over a series of subsystems or not. Inspecting the number of contributory causes of a risk in the CAM-C gives a sense of the level of dissipation or dilution.

Where an enumerated form of qualitative analysis is used for risk acceptance, as shown in Table 20. The suggested method of adjustment is to count the number of amplifiers in a path, adding one to a count for each. Next to count the number of resistors in a path, deducting one from the count for each. Finally, moving the category by the overall count for the risk in question to a higher frequency rate for a positive count and a lower rate for a negative count.

6.3.6 Quality control and troubleshooting a CAM analysis

Consistency checks should be made within the CAM method to sense check the analysis result. For example, replacing a high-level risk by the root causes or

lower-level causal risks that contribute to it, there should be some consistency in frequency, and consequence between the lower level causal risks and the high-level risk element. If after analysis the transformed lower level causal risk is far more frequent than the high-level element when referenced up to the top level through CAM-C, consideration should be given to the reasons why. Things to consider are:

- The parameters that define the causal risk are incorrect?
- The amplification in the CAM-C has over-exaggerated the actual effect to beyond a believable level.
- Is there a missing resistive link?
- The effect of the causal risk has not been realised before the CAM analysis.
- There is some deficiency in the system causing the effect.
- The high-level element has been underestimated.

Where there is an inconsistency which seems valid, it should be explained in the analysis report. For example, the exaggerated effect shown for the Grayrigg test case in Chapter 8 is explained by the effect of a lack of maintenance.

6.3.7 Developed CAM process

In summary, considering all the comments, there are distinct stages to CAM these are as follows:

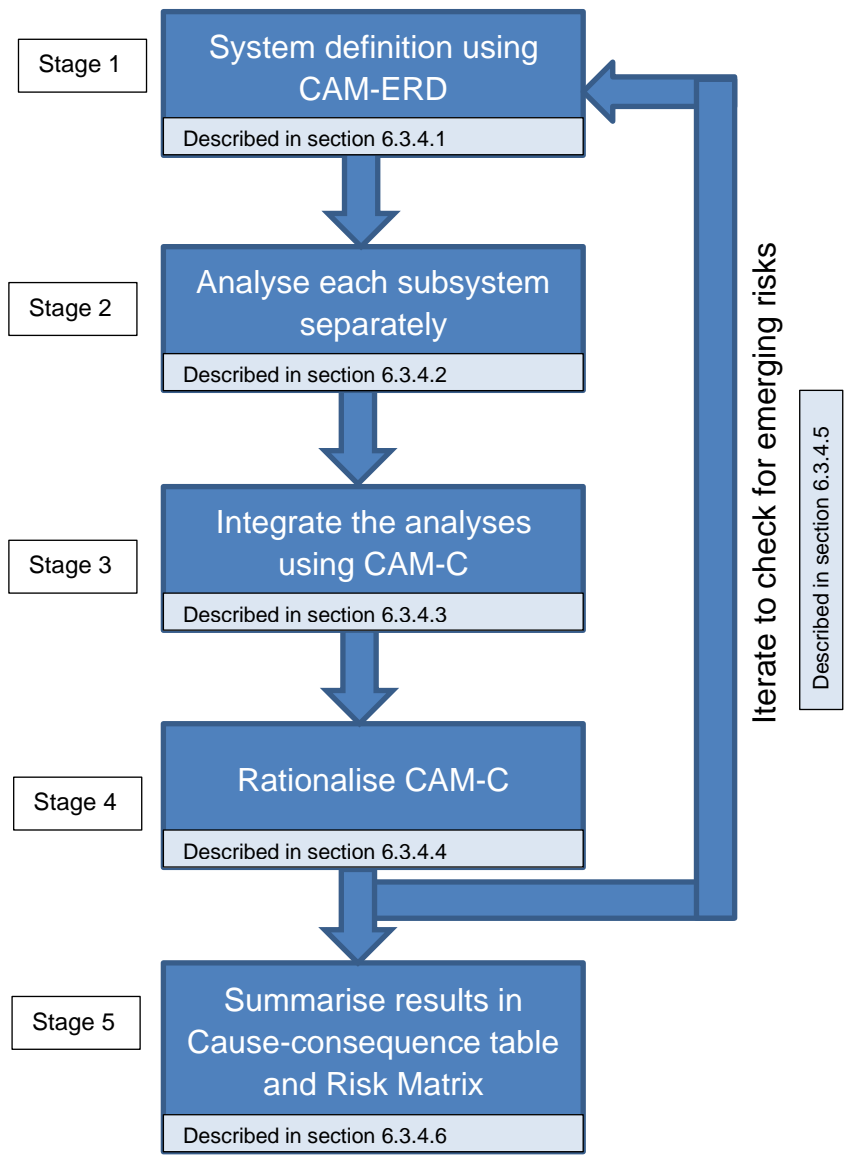


Figure 25 CAM process

Figure 25 shows the CAM process together with a reference to the descriptions of the process stages.


6.3.8 Method of choice for the subsystem analysis

Section 6.3.4.2 described how CAM allows for the use of existing methods to carry out the subsystem analysis. This section gives a guide how straightforward it is to use various techniques with CAM, some are easier to use than others.

Ease of use means that it fits into the CAM-C section of the analysis without much translation effort. The Author has weighed the results of the current technique analysis carried out in Chapter 4, Section 4.2. and applied a subjective approach

to the recommendation as shown in Table 21 because, in many ways, it is a personal preference for the practitioner.

Table 21 Ease of use recommendation



Technique	Comment
Cause-consequence	A tabulated form that fits with the CAM-C matrix and directly lists risks
FMEA	A tabulated form that fits with the CAM-C matrix. Ideally, failures need to be re-expressed in risk form in CAM-C
FMECA	A tabulated form that fits with a matrix. Ideally, failures need to be re-expressed in risk form in CAM-C
FTA	Pictorial view of the risk of a top event. Could require many FTAs to cover the scope. Each FTA maps only one top level event.
Reliability Block diagram	Pictorial view of the risk of a top event. Could require many RBD to cover the scope
Bow Tie	As per FTA and ETA as long as it is derived from them. Otherwise needs to be translated into a risk form and evaluated
Accimap	Data needs to be translated into a table.
SCM	Once events are identified the values can be used as part of the CAM-C
FRAM	The values from the model can be taken and used in the CAM-C
Bayesian Networks	The JPL values can be used in the CAM-C
ETA	Pictorial view of event outcomes. Could require many ETA to cover the scope and suitable for post-event consequence analysis only. The causal information is missing and would have to be supplemented through another technique.

6.4 Adaption of CAM for post-accident analysis

The scenario is that an accident has occurred and therefore risks have materialised. The objective of an analysis is to be able to explain why and prevent a reoccurrence. The Author has designed two schemes, a forward scheme and a reverse scheme.

6.4.1 CAM Post accident Forward Analysis – (FA)

The CAM process is slightly modified as shown in Figure 26, the modifications are shown in orange. The concept is to carry out a normal analysis and extract the relevant parts from it to explain the accident. The necessary alterations are described in the following paragraphs.

6.4.1.1 Stage A1 – list risks

The risks associated with the consequence are listed to provide the target for the analysis. The analysis should explain why these have occurred.

6.4.1.2 Stage A2 – Summarise causal risks

Extract the causal risks from the analysis and summarise them as the explanation of 'why' the accident has occurred. These are obtained from the CAM-C by identifying the causal risks from the columns that are linked to the risks listed in Stage A1. These are to be listed in the cause-consequence table first created in Stage 5.

6.4.1.3 Considerations when undertaking the analysis

- The CAM-ERD must describe the system as-is.
- After the generation of the CAM-C it is not necessary to carry out a rationalisation.

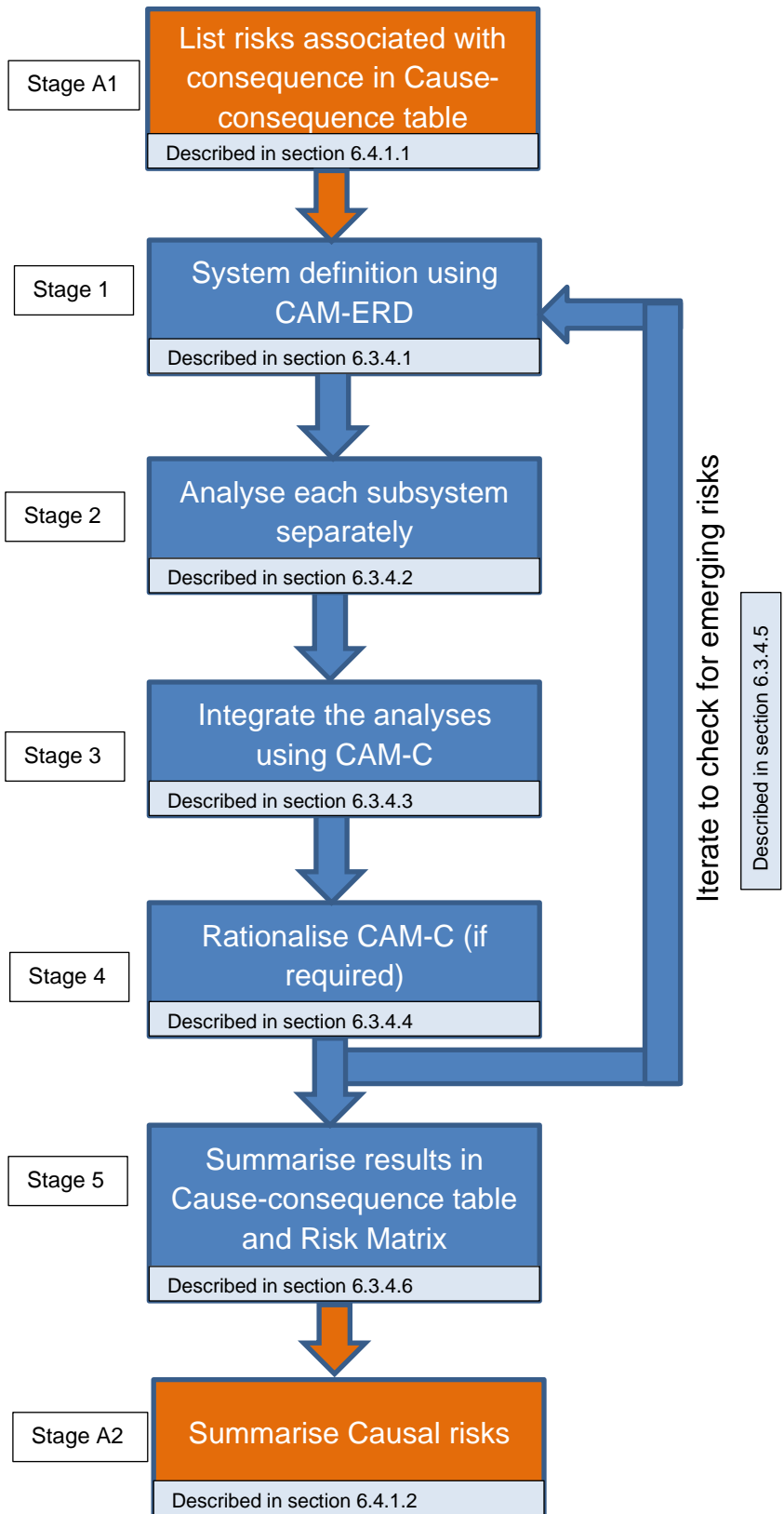


Figure 26 CAM adapted for post-accident analysis in the forward direction

6.4.2 CAM Post accident Reverse Analysis – (RA)

The CAM process is slightly modified as shown in Figure 27, the modifications are shown in green. The concept uses the generated risks from the accident and uses CAM in reverse to decompose these into causal risks and therefore explain the accident. A number of the stages in the normal CAM process are not required because the CAM process is tracking a line of causes rather than generating possible outcomes. The necessary alterations are described in the following paragraphs.

6.4.2.1 Stage B1 – Initial system CAM-ERD

The information provided from an incident is used to form an initial view of the system to be assessed. The objective is to obtain enough of an understanding of the system to populate the list risks in stage B2. The CAM-ERD is drawn up in the same manner as described in Section 6.3.4.1, the difference is that there may only be partial information available at this stage of the analysis.

6.4.2.2 Stage B2 – list risks

The risks associated with the consequence are listed in a cause-consequence table to provide the list of risks for the analysis in Stage B3.

6.4.2.3 Stage B3 – Create CAM-C for system risks

Use the list of risk from Stage B2 to create a CAM-C with the consequences as the row entries and the risks as the column entries. The cells linking the risks and consequences are to be filled in, mapping the consequences to risks. The entries in this case are a simple “yes” to indicate where a link exists.

A further column should be inserted in the CAM-C headed “evidence”. Where there is evidence to support the link a “yes” should be inserted in the cell.

6.4.2.4 Stage B4 – Decompose the risks using CAM-C in reverse

The CAM-C is developed by constructing the CAM-C in reverse, using the trace method explained in Section 6.3.4.3 in a slightly modified form. In this particular case the column entries are generated by the analyst using information from the CAM-ERD. The cell values are filled in as usual to reflect the existence of links and the type of link. The analyst continues with this process until enough detail has been generated about the causal risks.

At each stage the cause-consequence table is updated to reflect the uncovered risks and remove those that are of no interest i.e. where there is no evidence

6.4.2.5 Stage B5 – Summarise causal risks

Extract the causal risks from the analysis and summarise them as the explanation of 'why' the accident has occurred. These are obtained from the CAM-C by identifying the causal risks from the columns that are linked to the risks listed in Stage B2. These are to be listed in the cause-consequence table first created in Stage 5.

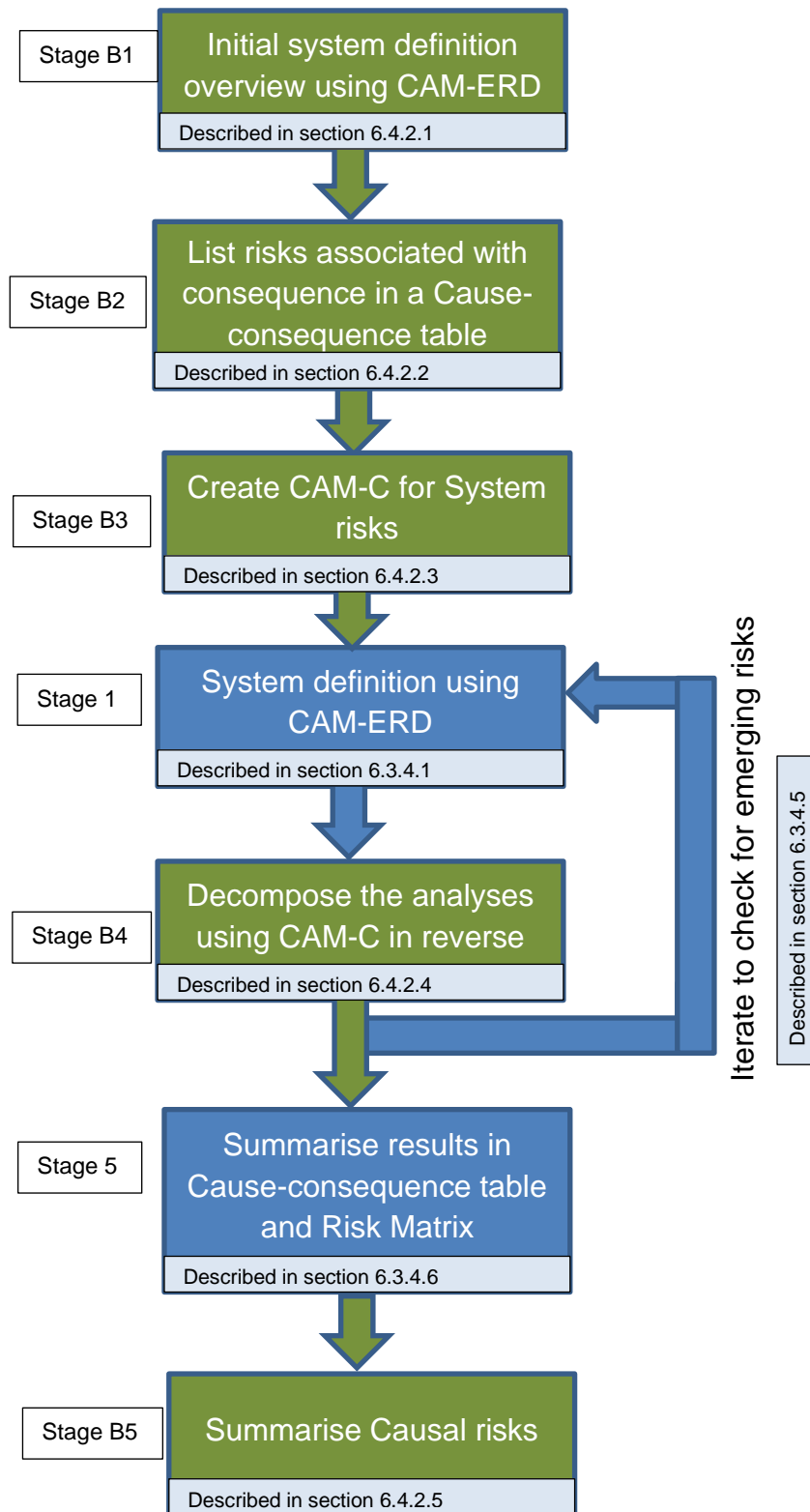


Figure 27 CAM adopted for accident analysis in the reverse direction

6.5 The three configurations of CAM

Figure 25, Figure 26 and Figure 27 can be combined into a unified full CAM method, as shown in Figure 28, which contains the three flows previously developed. Going forward, the shorthand in this thesis is as follows:

Table 22 Shorthand name definition

Method	Flow diagram	Figure 28 diagram colour	Shorthand name
Forward New/novel/modified system method	Figure 25	Green	CAM_FN
Forward accident method	Figure 26	Orange	CAM_FA
Reverse accident method	Figure 27	Turquoise	CAM_RA

The stage numbers on the diagram refer to the sections in the main text. As can be seen there is a lot of common processes between the three variants.

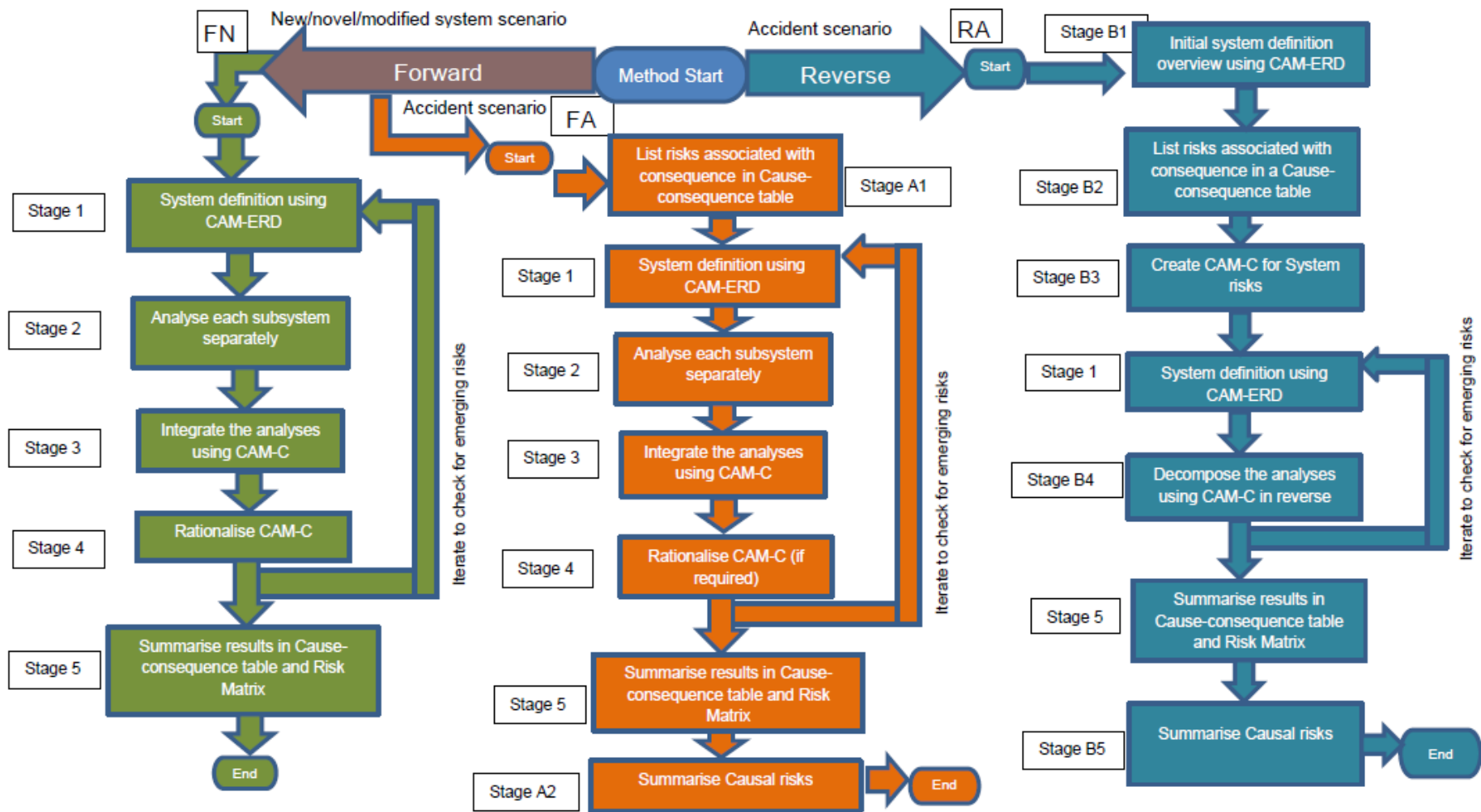


Figure 28 Combined CAM method flow diagram

6.6 Simple demonstration

This simple demonstration of CAM uses the Forward Novel (FN) mode as described in section 6.3.4 to illustrate how to apply CAM. The chosen method of subsystem analysis is FMEA for this demonstration.

This is a simplified examination of a shortcut path which was installed on a new housing estate designed to fit the architectural feel of the estate, as described in detail in Appendix C. Natural materials were used to create a countryside image. The effect was a green area with existing trees in the centre and a path at the side next to a private drive. The shortcut is used by cyclists. When the weather is bad rain cascades down the path washing some of it away leaving an uneven surface and exposed water meters in the path.

6.6.1 Risk acceptance

A semi-qualitative method of assessing risk is used based on EN50126 (CENELEC, 2017), shown in Table 23. The matrix has been calibrated by the Author to make it suitable for the example using the principles put forward by HSE (Health and Safety Executive, 2001) to set levels for risk acceptance in terms of likelihood (rows) and consequence (columns).

Table 23 Risk matrix formulated from (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic	
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable	<1wk
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable	<1mth
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable	<6mth
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable	<1yr
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	<2yrs
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	≥2yrs

Green areas are deemed 'broadly acceptable', yellow areas are 'tolerable' and the red areas are 'intolerable'.

6.6.2 Stage 1

The first task is functional decomposition by structural systems and behavioural flow using a CAM-ERD to map the relationships.

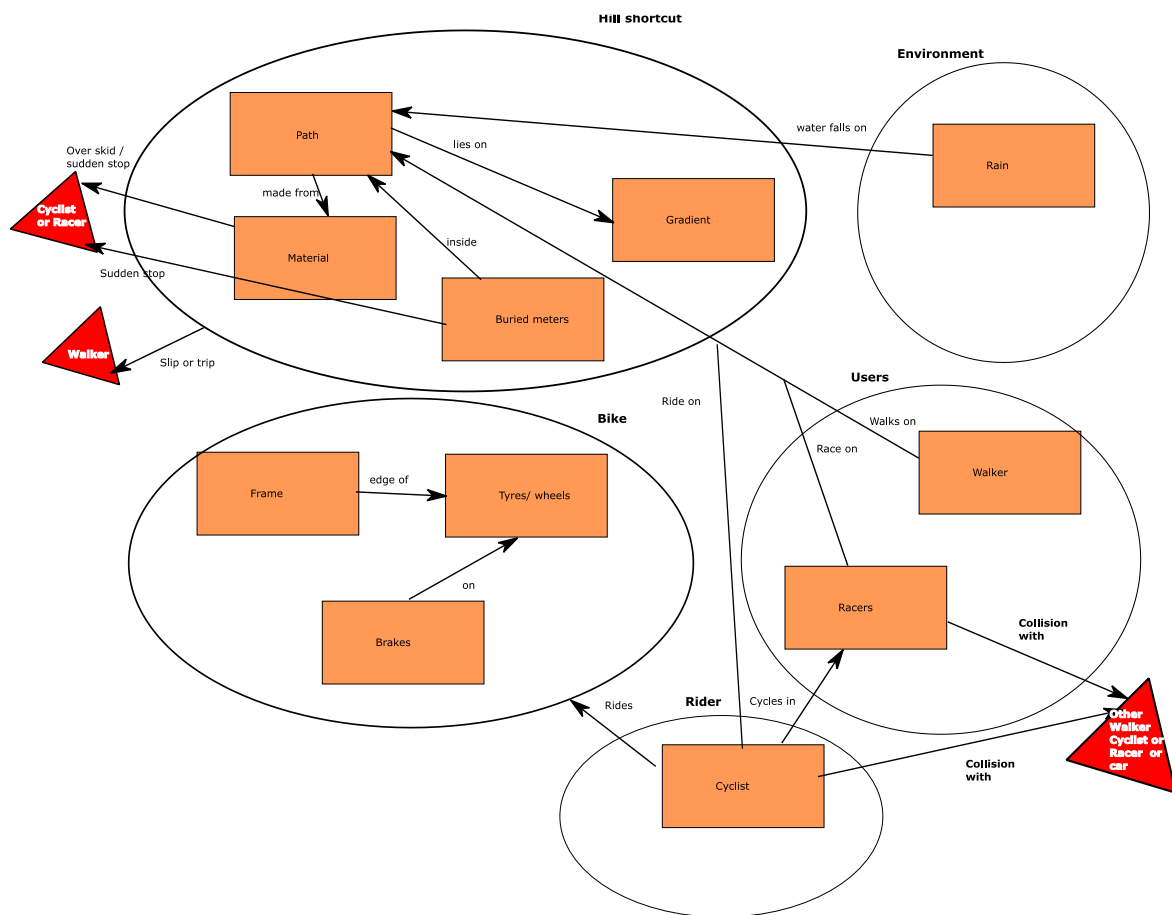


Figure 29 CAM-ERD Relationship diagram

Figure 29, shows the CAM-ERD created by the Author for hill shortcut system which is dependent on the properties of the path for safety. The nominal subsystems are shown in circles. Note effectively the cyclist is the top-level subsystem. The other systems impact the safety of the cyclist in various ways.

The parts of the subsystems are shown in rectangles and the perceived risks on

the arrows together with a few additional association notes. The point of harm is highlighted by the triangle.

6.6.3 Stage 2 – subsystem analysis

The chosen method for the analysis is FMEA which has been conducted using EN60821 (CENELEC, 2006) and Anleitner (2010) and tailored to a safety application in a similar way to Mohr (2002). The approach has been to treat the systems as performing a function and then to document the failure of the function. A high detection number of 10 indicates that it will be easy to detect and prevent through the applied controls, conversely a low score indicates that the failure is difficult to detect and therefore may be latent. The classification is S for a significant function failure and C for a critical failure where there is a direct safety implication. Classification conversions, if necessary, from S to C are performed by adjusting the occurrence to reflect that not every failure will result in a safety event as articulated by Lepmets (2017). Also, consideration will be taken of the effect of detection and controls when setting the occurrence in the case of a safety classification. The RPN field is not considered appropriate for this particular application.

The scale for the severity and conversion of the frequency to a scale used in the risk matrix are given in Table 24 and Table 25 below in preference to the normal 10-point scale.

Table 24 Scaling table for occurrence formulated from (CENELEC, 2017)

Occurrence Category	Value	Definition
Frequent	6	Less than a week
Probable	5	Less than a month
Occasional	4	Less than 6 months
Rare	3	Less than a year
Improbable	2	Less than 2 years
Highly Improbable	1	Greater or equal to 2 years

Table 25 Scaling table for the severity formulated from (CENELEC, 2017)

Category	Value	Safety Definition	Equipment failure definition
Catastrophic	5	Multiple fatalities	Multiple systems loss
Critical	4	Fatality/multiple major injuries	Major loss of system
Major	3	Life changing injury	Severe systems damage
Marginal	2	Injury	Minor systems damage
Insignificant	1	No material harm	

Table 26 FMEA for Hill shortcut (shortcut and environment)

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
101	Path	Solid foot way	Failure during operation	Path breaks up	Uneven surface And exposed meters Tripping likely	2	S	Water drainage	1m	Choice of material	Inspection and surveys	8		If the path is washed away the buried service equipment may be exposed. Furthermore, it will be difficult to function as a walkway.
104	Material	Stable even surface	Failure during operation	Material washed away	Uneven surface And exposed meters Tripping likely	4	S	Water flow downhill causing scouring	1m	Choice of material packing and containment	Inspection and surveys	5		This is water volume/flow and materials dependent. However, current performance shows that the path material is susceptible to water flow.
105	Material	Solid surface	Failure during operation	Material does not support load	Uneven surface	2	S	Material too soft (sand) instead of rock based	1m	Choice of material design codes	Construction inspection and surveys	5		This is materials dependent. If the material is too soft then bikes will create ruts.
106	Buried service	Meter top to be flat with path	Failure during operation	Exposed meter head above ground level	Tripping hazard	3	C	Surrounding material not solid	1m	Design codes	Inspection and surveys	4		Meters need to be accessible which means the top has to meet the surface of the path. Detection is not so easy in the dark if they are proud of the path surface level.

Table 27 FMEA for Bike

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
201	Frame	Support components of bike	Failure during operation	Structural failure	Bike falls apart	4	S	Welds giving way due to fatigue	5yr	Design and manufacture	Quality inspection and reports	3		Depends on the quality of the bike, but they are supposed to be made to standards.
202	Brakes	Stop bike	Failure during operation	No friction	Bike does not stop	3	C	Worn out	10yr	Service and maintenance	Maintenance	7		It is unlikely that both sets of brakes (front and back) will be worn out at the same time.
203	Brakes	Stop bike	Failure during operation	No friction	Bike does not stop	3	C	Contamination	10yr	Cleaning and design to clean through friction	Maintenance	2		In much the same way as any friction brake. The contact with the rim of the wheel will tend to clean the surface.
204	Tyres	Grip	Failure during operation	Loss of grip	Bike falls over	2	C	Slippery surface	1yr	Rider experience	Experience	8		

Table 28 FMEA for Rider process

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
301	Cyclist	Ride along path	Failure during operation	Fall off	Injury to legs	2	C	Unbalanced or uneven surface or obstacle	1yr	Experience	Experience	2		This could be due to a misjudgement, a mechanical failure of some kind or hitting an obstruction.

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
302	Cyclist	Stop before hazard	Failure during operation	Fail to stop	Run down	4	C	Misjudgement	5yrs	Experience	Experience	2		The rider either hits the obstruction or is placed in a place where could he hit
303	Cyclist	Skid stop	Failure during operation	Bike skids away	Injury to legs	2	C	Loss of grip	3m	Experience	Experience	2		Not every skid loss of control will result in injury
304	Cyclist	Control bike	Failure during operation	Mechanical failure	Injury to legs	2	C	Components break on bike	5yr	Bike design, maintenance	Maintenance	5		Most things could be spotted and corrected before they become a problem
305	Cyclist	Stop before hazard	Failure during operation	Mechanical failure	Injury to legs	3	C	Components break on bike	2yrs	Bike design, maintenance	Maintenance	5		Most things could be spotted and corrected before they become a problem

6.6.4 Stage 3 – integrate the analysis

This section describes the integration from FMEAs into a CAM-C. Numbers are inserted in intersecting cells where there is a link between the risks. For example, the Author has assessed that if material is washed away (104) there is an amplified risk that a meter will be exposed above ground level (106), hence a value of 3. Likewise, the Author has judged that a structural failure of the bike could cause the rider to fall off. However, this is unlikely because bike frames are well made and if a failure occurred it is likely to be spotted well before it became dangerous. This link has been designated as a terminator because the likelihood that a structural failure could happen is vanishingly small in the time frame of the analysis. Risk 302 has been designated as partially described (denoted by PD) because the failure to stop is partly a property of the bike but also a property of the cyclist in the shape of misjudgement. Risks 202 to 204 have no causal risks in the model because they are root causal risks in this model. Risks 304 and 305 are summarising risks for bike mechanical failures arising from 201, 202 and 203, and in this case 304 and 305 are used for the analysis.

Table 29 CAM-C

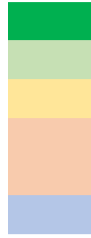
		Path breaks up	Material washed away	Material does not support load	Exposed meter head above ground level	Structural failure	No friction	Loss of grip	Fall off	Fail to stop	Bike skids away	Mechanical failure
		101	104	105	106	201	202 203	204	301	302	303	304 305
101	Path breaks up		2	2								
104	Material washed away											
105	Material does not support load											
106	Exposed meter head above ground level	3	3									
201	Structural failure											
202 203	No friction											
204 206	Loss of grip											
301	Fall off	2	2	2	3	-10		2			2	2
302	Fail to stop									PD	2	
303	Bike skids away											
304 305	Mechanical failure					2	2					

6.6.5 Stage 4 - rationalisation

The CAM-C generated in stage 3 is annotated with colour to show the rationalisation in Table 30. Those causal links that link within a subsystem are eliminated from further analysis (shown in orange). The terminator link (shown in yellow) is also eliminated. There are no duplicate links to be removed. A number of links have been signified as summary links (blue). This designation is where the causal risk is really a summary (includes) the other causal risks. For example, risk 101 is really a summary of 104 and 105. The summary links for the path are not considered further in the analysis, otherwise there would be double counting of risks, while 304 and 305 are used in preference to their causal risks.

Table 30 Rationalised table

- System level item
- remove effective duplicates
- eliminate terminators
- remove links that do not affect system of interest
- signify summary links



		path breaks up	Material washed away	Material does not support load	Exposed meter head above ground level	Structural failure	No friction	Loss of grip	Fall off	Fail to stop	Bike skids away	Mechanical failure
		101	104	105	106	201	202 203	204	301	302	303	304 305
101	Path breaks up		2	2								
104	Material washed away											
105	Material does not support load											
106	Exposed meter head above ground level	3	3									
201	Structural failure											
202 203	No friction											
204	Loss of grip											
301	Fall off	2	2	2	3	-10		2			2	2
302	Fail to stop									PD	2	
303	Bike skids away											
304 305	Mechanical failure					2	2					

The nominated system level risks are chosen by considering the point of harm in the CAM-ERD, which relate to falling off or failing to stop and hitting something. These are highlighted in green in the annotated CAM-C. These risks are now the focus of the analysis.

6.6.6 Stage 5 – summarise the output

Table 31 is used to list all the relevant FMEA entries. To obtain the level of adjustment required two columns are added to the right-hand side of the FMEA. As described in Section 6.3.5. for every amplifier a count in these columns is incremented by one. In this case 106 is amplified at the system level incurring a count of 1. As previously described the frequency is roughly doubled (in red).

The FMEA rows in Table 31 are translated into the cause-consequence table, Table 32, by looking up values from Table 24 for the occurrence and placing the enumerated value in the likelihood column. Likewise, the consequence is obtained from Table 25 and interpreting the 'potential failure effects' column in the FMEA matrix, a similar interpretation is use to obtain the entry in the consequence description column of the cause-consequence table. Finally, the risk is obtained from Table 23.

Table 31 Combined FMEA

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Adjust sys level 301	Adjust sys level 302
104	Material	Stable even surface	Failure during operation	Material washed away	Uneven surface And exposed meters Tripping likely	4	S	Water flow downhill causing scouring	1m	Choice of material packing and containment	Inspection and surveys	5		Water and materials dependent	0	
105	Material	Solid surface	Failure during operation	Material does not support load	Uneven surface	2	S	Material too soft (sand) instead of rock based	1m	Choice of material design codes	Construction inspection and surveys	5		Materials dependent	0	
106	Buried service	Meter top to be flat with path	Failure during operation	Exposed meter head above ground level	Tripping hazard	3	C	Surrounding material not solid	4m 2wks	Design codes	Inspection and surveys	4		Meters need to be accessible which means the top has to meet the surface of the path. Detection is not so easy in the dark	1	
202 / 203	Brakes	Stop bike	Failure during operation	No friction	Bike does not stop	3	C	Worn out/contamination	10yr	Service and maintenance	Maintenance	7				
204	Tyres	Grip	Failure during operation	Loss of grip	Bike falls over	2	C	Slippery surface/wrong tyres	1yr	Rider experience	Experience	8			0	

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Adjust sys level 301	Adjust sys level 302
301	Cyclist	Ride along path	Failure during operation	Fall off	Injury to legs	2	C	unbalanced	1yr	Experience	Experience	2				
302	Cyclist	Stop before hazard	Failure during operation	Fail to stop	Run down	4	C	Misjudgement	5yrs	Experience	Experience	2				
303	Cyclist	Skid stop	Failure during operation	Bike skids away	Injury to legs	2	C	Loss of grip	3m	Experience	Experience	2			0	0

Table 32 System cause-consequence table

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Control	Evaluation type	Likelihood	Consequence	Risk
301-104 (R1)	Fall off	Unbalanced	Path material washed away	Heavy rain washes material away and leaves uneven surface	Rider loses balance and falls off	grazed leg	Path maintenance	Risk Estimation	Occasional	Marginal	Tolerable
301-105 (R2)	Fall off	Unbalanced	Path material not suitable	Path rutted	Rider loses balance and falls off	grazed leg	Path design	Risk Estimation	Occasional	Marginal	Tolerable
301-106 (R3)	Fall off	Unbalanced	Exposed meter head	Meter head is above path and is hit by bike wheel	Rider loses balance and falls off	Broken leg	Path design and maintenance	Risk Estimation	Probable	Major	Intolerable
301-204 (R4)	Fall off	Unbalanced	Loss of grip on tyres	Tyres lose grip on the surface	Rider loses balance and falls off	grazed leg	Experience	Risk Estimation	Rare	Marginal	Negligible

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Control	Evaluation type	Likelihood	Consequence	Risk
301-303 (R5)	Fall off	Unbalanced	Misjudged skid	Rider misjudges the amount of skid and bike falls away	Rider loses balance and falls off	grazed leg	Experience	Risk Estimation	Occasional	Marginal	Tolerable
302 (R6)	Fail to Stop	Hit obstacle	Misjudgement in braking	Rider misjudges the braking distance and hits obstacle	Rider is thrown off the bike	Broken leg	Experience	Risk Estimation	Highly improbable	Major	Negligible
302-303 (R7)	Fail to Stop	Hit obstacle	Misjudged skid	Rider misjudges the amount of skid and bike falls away when the wheel hits an obstacle	Rider loses balance and falls off	grazed leg	Experience	Risk Estimation	Occasional	Marginal	Tolerable

The values in Table 32 are translated in the risk matrix of Table 33 using the shortened risk names (Rx). As can be seen a single risk R3 is deemed unacceptable.

Table 33 Analysis summary risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					
Probable			R3		
Occasional		R1, R2, R5, R7			
Rare		R4			
Improbable					
Highly Improbable			R6		

6.7 Summary

This chapter has described the justification to develop CAM based on the information from previous chapters 2, 4 and 5. CAM has been developed and described in Section 6.3 of this chapter using insights gained in previous chapters, this version of CAM is optimised for a design or alteration scenario. Two further variations of CAM have been developed in Section 6.4 to address risk assessment of accident scenarios where the requirement is to trace back from an event to causes.

A simple example has been provided to demonstrate how CAM can be applied in practice.

Chapters 7, 8 and 9 apply CAM to various test cases to provide assurance that CAM is a valid risk assessment process, as was described in Chapter 1 Section 1.9. A set of CAM user instructions have been created in Appendix J with illustrations and process steps, these instructions are used to carry out the test cases of chapters 7-9.

6.8 Principal points

The principal points from this chapter are as follows:

- i. A new safety risk analysis method, CAM, has been justified, developed and explained.
- ii. Two variants of CAM have been developed and optimised for accident investigation. These use common parts of CAM and the three together form the CAM risk analysis suite.
- iii. An example application of CAM has been demonstrated.

7 Baildon Rail based comparative analysis case study

This chapter provides part of the validation assurance for the CAM safety risk analysis method created in Chapter 6. It contains a single case study that takes an example incident, Baildon (Rail Accident Investigation Branch, 2017), and applies three different analysis methods, including CAM, and compares the relative performance of each. The RAIB report provides a reference to validate CAM against. Also, it serves as a demonstration that CAM can be successfully applied to railway risk assessment.

The RAIB incident review described in Chapter 5 has indicated Baildon is a representative multisystem incident.

The case study splits into two main sections, the first, Section 7.3, illustrates the application of CAM as a test case in the forward mode and compares the results with the official incident report Rail Accident Investigation Branch (2017); success is deemed as CAM identifies at least the same causes as the RAIB report. The second, Section 7.4, compares the results and experience from the application of CAM, Yellow Book, and STAMP analysis methods to the Baildon incident. In this case, each of the methods is used in their 'forward' analysis mode.

The first part of this chapter, Section 7.3, describes the application and development of CAM as initially proposed, as part of the test case. Before moving on to Section 7.4 and a comparison with other methods, corrections were applied to CAM.

7.1 Assessment of risk

For these test cases, a semi-qualitative method of assessing risk has been used by the Author based on EN50126 (CENELEC, 2017), shown in Table 34, as a

calibrated likelihood-consequence risk table to perform a qualitative risk assessment evaluation. It is used to allocate and identify the acceptable levels of risk based on the Author’s predetermined thresholds that align with the ORR guidance (Office of Rail and Road, 2018).

Table 34 Calibrated risk matrix based on (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic	
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable	<1yr
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable	<2yrs
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable	<5yrs
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable	<10yrs
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	<20yrs
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	≥20yrs

The green areas represent the ‘broadly acceptable risks where further mitigation is not required, the yellow are ‘tolerable’ risks where risks are required to be mitigated to an ALARP level, while the red are ‘intolerable’ risks are not acceptable. Each cell is a combination of likelihood (row) and consequence (column).

7.2 Use of RAIB reports in the analysis

The Author uses the findings of the RAIB reports as a reference of well-founded statements to measure the test case analyses against. Also, the incident descriptions and investigation commentary are used as input data for the test cases. These are regarded as statements of fact.

The Author decided that this is a valid position because:

1. The draft reports are reviewed by stakeholders in the industry such as RSSB and Network Rail before publication.
2. Other academics cite the reports.
3. The ORR enforces the recommendations.

The first reason indicates that reports are subject to correction and acceptance within the industry by knowledgeable stakeholders, increasing confidence in their accuracy. Reason two indicates that there is widespread academic acceptance of the quality of the reports. For example Underwood and Waterson (2013b) bases a benchmarking exercise on RAIB data, Zhou and Yan (2018) use RAIB data as a reference and state “RAIB analysis is more of an objective analysis and explanation as the third party in terms of the accident”, and Kim and Yoon (2013, p.58) states “The RAIB accident reports were used because the RAIB provides more comprehensive and detailed reports than other accident investigation agencies such as the U.S. Federal Railroad Administration (FRA)”. Finally, reason three logically indicates that the findings and recommendations must be accurate otherwise it would not be possible to for ORR legally enforce them.

However, it is not possible to go further and use extracts from the RAIB analysis because the approach RAIB take to investigation analysis is unclear from publicly available information. The RAIB objective is to identify the root and subsidiary causes, which allow recommendations to be formulated. These recommendations are formulated against ALARP criteria to prevent reoccurrence, as described by Rail Accident Investigation Branch (2014). It is unclear from RAIB material how risk analysis is undertaken. The methods webpage (Rail Accident Investigation

Branch, 2014) indicates that it collects evidence, carries out interviews and carries out reconstructions. It does not expand on the techniques for investigation and understanding what happened. Therefore, the Author has no insight into these intermediate steps but is confident that the outputs are robust.

7.3 Baildon desktop test case application

This application is a test case study carried out to benchmark the CAM analysis method and validate the output using the publicly available information, which is limited. The RAIB has investigated Baildon and produced a report by Rail Accident Investigation Branch (2017) of their investigation. The report has been used as the source of information for the case study and it provides a reference to compare with the CAM findings.

Appendix G describes the full CAM analysis; a summary of the key points from the CAM application is explained in this chapter subsection. It includes a discussion and justification of the process steps.

The scenario report, Appendix D, presents a single system, the railway, that has been affected and it could be concluded that this does not fit with the hypothesis of a connected system. However, this analysis reviews the other 'upstream' systems to identify any connectivity where a failure of any of these systems impacts the railway system concerned and decomposes the railway into salient subsystems to yield a greater understanding.

The analysis has been simplified to enable the rapid development of the method. Given the limited detail available, hazard identification has been limited in this case to the essential facts.

7.3.1 Test case success criteria

The measures of success for a case study were defined in Chapter 1 Section 1.9 as Safety, Economic and Applicability, which for this case are interpreted as shown in Table 35.

Table 35 Success measure interpretation

Measure	Interpretation
Safety	The CAM analysis outcome should at least include the same 'answer' as the official report, and if there are other factors, it should identify these too.
Economic	The process should be understandable and relatively effortless to implement without resort to specialist tools, such as specialist software packages or high-powered computers. Also, it should be possible to complete the analysis with a reasonable timeframe; 5days. Furthermore, the analysis should be less than 50 pages.
Applicability	The process should be directly applicable to the railway environment without additional adaption.

The first measure is factual, the second is a mixture of factual and subjective while the latter measure is subjective. Subjective measures are demonstrated through illustration and success is judged subjectively by the Author.

7.3.2 Method used

The analysis method used is as explained in Chapter 6, Section 6.3.4 and labelled as CAM-FN (Forward New/novel/modified analysis). The process is reproduced in Figure 30 for convenience and the user instructions can be found in Appendix J. The Author has decided for the purposes of this test case that the CAM-FN variant is more appropriate than the accident variants because the objective is to see if a CAM analysis produces a set of outputs rather than attempt to trace the causes from an incident.

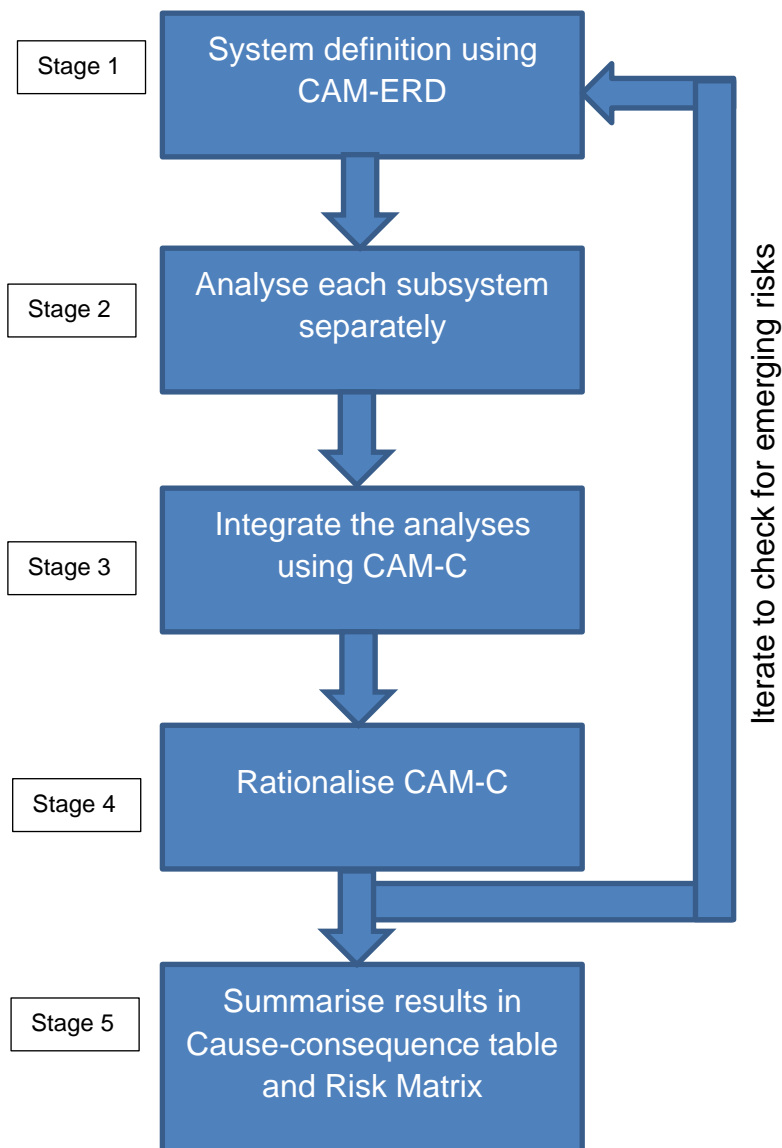


Figure 30 CAM_FN process reproduced from Chapter 6

For this analysis FMEA has been selected as the method for the subsystem analysis because it was found to be the most popular from the industry analysis in Chapter 4.

The boxed 'Stage' labels in Figure 30 refer to stages in the process which are described in Appendix J. These labels are also used in this section as bold underlined headers to indicate the part of the process that is being described.

7.3.3 Information from the RAIB report

The information below is summarised from the RAIB report (Rail Accident Investigation Branch, 2017) into the Baildon incident to provide a context for the analysis.

7.3.3.1 Brief summary of the incident

A full summary and diagrams relating to this near miss incident are shown in Appendix D.

During heavy rain on 7 June 2016 part of the structure supporting the railway line was washed away by floodwater flowing down an embankment. The incident was reported by members of the public and the Fire and Rescue service to controllers at Network Rail, who took no effective action and several trains passed over an unsupported section of track. The report focuses on the failings of Network Rail in dealing with the reports. The concern expressed by the RAIB report is that the incident could have easily resulted in a derailment and consequential injuries and fatalities.

7.3.4 List of failures identified from RAIB report

Table 36 Extracted list of causal factors from RAIB report

Ref	Primary causal factor	Secondary causal factor
1	Ballast under one rail washed out	<ul style="list-style-type: none"> a. Drainage could not cope with the quantity of floodwater b. Flood water directed onto a single-sided embankment c. Previous flood repair did not withstand water flow
2	Reports of track damage not dealt with appropriately	<ul style="list-style-type: none"> a. Controllers did not listen carefully to emergency calls b. Controllers misdirected responders to a different location c. Responders not aware of the vulnerability of embankment to flooding d. A third train was allowed to traverse the washed-out track section when the line was blocked

The Author has drawn a number of initial impressions from the findings to help frame the analysis:

1. There are in effect three events; first, there is a washout, second trains traversed the washed-out section of the line and finally, a train traversed the washout after it should have been stopped. These are sequential, and therefore like Heinrich (1931) dominos, cited by Reason, Hollnagel and Paries (2006), the removal of any one of them will stop the follow-on events in the sequence.
2. Logically considering the risk of an accident, it will only occur when the train operates over the washed-out section. Therefore, the operation of further trains is not really of concern regarding the primary incident as the risk has already materialised. Prevention of the transit of further trains only prevents a reoccurrence of the materialisation of the risk.

Table 37 List of failure findings from RAIB report related to the washout event

Finding	Post or pre-event finding
Wrong section inspected / section missed.	Post event
Track washed out for 4m.	Event
Drainage could not cope.	Pre-event
The previous washout had been repaired.	Pre-event

7.3.5 Analysis

The CAM analysis undertaken by the Author is fully described in Appendix G; this section contains summarised key points and commentary to illustrate the application of CAM and its features. The steps used for the analysis are described in Chapter 6 and reproduced in as a set of instructions in Appendix J.

CAM-Stage 1 CAM-ERD

Key points summary

The first task is to understand the composition and the boundaries of the system. The composition detail can then be used to split the system into analysable parts.

The decomposition has been performed using a CAM-ERD and is reproduced in Figure 31. This diagram is described in Appendix G and is a mixture of physical and process risk flows. The major subsystems are indicated by circles while the parts are indicated by rectangles. The point of harm is indicated by a red triangle. Relationships are shown as arrows. As can be seen, the interrelationships are identified. Furthermore, the interface to a potential accident is clearly identified as a derailment.

The CAM-ERD has been constructed from the incident material provided by RAIB (Rail Accident Investigation Branch, 2017) and distilled into a set of incident facts in Appendix D¹⁷ using the instructions from Appendix J.

¹⁷ The reason for this approach is to ensure that all the different analyses (CAM, Yellow Book, STAMP) use the same set of facts as the starting point to reduce the likelihood of bias.

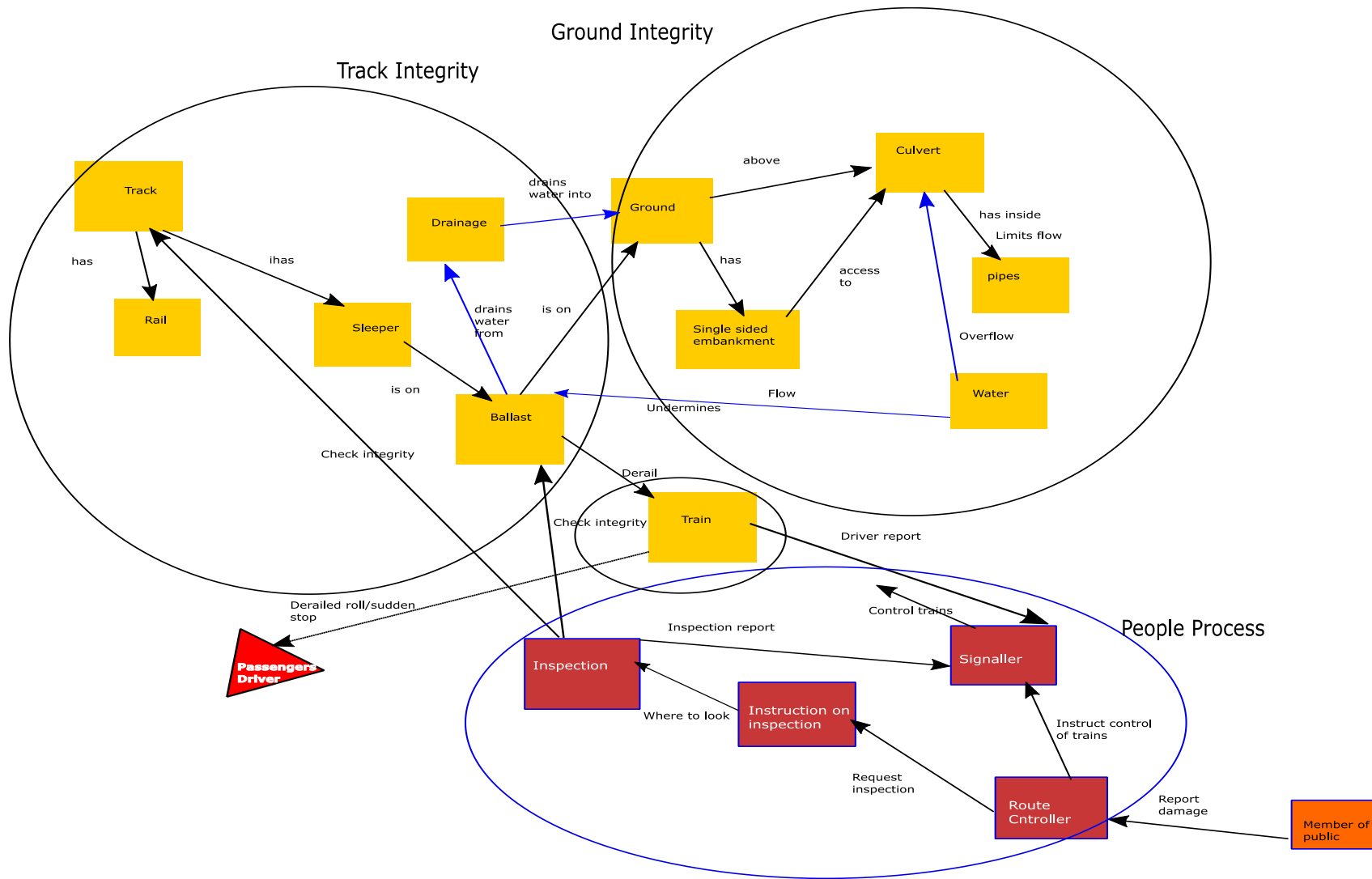


Figure 31 CAM-ERD relationship diagram from Appendix G

Commentary

The creation of Figure 31 came about after several attempts of sketching on paper. Critical considerations were deciding where the functional separations are into subsystems. Originally this stage was performed without the subsystem boundaries. After establishing the primary relationships, the parts were moved to appropriate subsystem groupings. Constructing a table of candidate subsystems and features helped clarify the understanding and subsystem linkages. The resulting diagram appears to provide a set of justifiable subsystems and identifies the interfaces between the parts. Consequently, there is a foundation for stage 2 of the analysis.

The overall system has been broken down into several subsystems. The Author has selected the FMEA technique for subsystem analysis, Appendix G contains a FMEA for each subsystem. FMEA was used because it was the most popular from the industry survey carried out in Chapter 4. FMEAs have been carried out from a safety analysis perspective.

CAM-Stage 2 subsystem analysis

Key points summary

The FMEA analysis has been created using EN60821 (CENELEC, 2006) and Anleitner (2010). Table 38 shows an extracted example. The right-hand two columns are used as verification of the entries against the source data (Appendix D). Lepmets (2017) has described that FMEAs will identify the causes of failures which are equivalent to those in a hazard analysis. Yet, hazards are not readily

identifiable from an FMEA because not all failures result in a hazardous situation, the CAM-ERD and CAM-C have been used to assist, as described later.

The example FMEA shows two entries that are part of a contributory subsystem. In this case, item 104 has a high impact on flooding, but is not readily apparent at this stage. In contrast, item 103 indicates there is a safety implication from the failure. No rationalisation of the data happens at this stage of the analysis. The next stage of CAM, CAM-C uses all of this information to capture a rich set of input, and consequently there will be less chance of missing key items. This is made possible in CAM by conducting an FMEA analysis for each subsystem identified in the CAM-ERD.

Commentary

While selecting FMEA for the reasons above, it became clear that it was reasonably straightforward to populate the tables. It was achieved by referring to the CAM-ERD and using the facts from Appendix D. As an established technique, FMEA provides a simple summary of the failures in each subsystem.

The issue noted with FMEA use was the large volume of data required.

Furthermore, classifying the entries between c critical and s significant was the reverse of a natural association. Finally, extending some periods to reflect the influence of mitigations, such as the rulebook requirements, lowered the failure rate from a safety perspective.

The failures conversion to hazards was deferred to a later stage of the process because it is more convenient when the relationships are simplified.

Table 38 Extract of FMEA for ground integrity (culvert and environment)

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
103	Culvert	Support the ground above	Failure during operation	Structural collapse	Land subsides	Possible derailment and injuries	4	C	Too much weight on the structure	20yr	Design codes	Reports from railway	5		The culvert will cease functioning	1	1
104	Culvert	Water volume flow	Failure during operation	Water leaks out of inspection manholes	water flows down the embankment	Water lows along the railway	2	S	Pressure too high as a result of too higher volume	20yr	Control of pressure and flow volume	Reports from the surrounding area and calculations	5		The pressure forces the water to rise up the inspection manholes and pop the covers. If this happens, water flows down the embankment and over the railway.	2	3

The CAM Combinator (CAM-C) – Stage 3

Key points summary

Table 39, is reproduced from Appendix G. The convention adopted is that inputs are columns and outputs are rows, is described in Appendix J. This convention is interpreted as the columns acting as causes for the hazard or failure indicated in the rows. This particular CAM-C has been formed by taking the failures from the FMEA entries to create the single view for the whole system and then convert this to a cause-consequence table later in the process, as described in Appendix J. The CAM-C entries have been organised by grouping the failures around subsystems as indicated in the CAM-ERD. Consequently, the comments on this section of the process refer to failures rather than hazards.

Commentary

The construction of the CAM-C diagram was reasonably straightforward when using the CAM-ERD as a guide on how the matrix should be laid out and grouped into subsystems. The data points were extracted from the FMEAs with the CAM-ERD used to help understand the path and estimated using the CAM-C rules. Estimating the link value required a qualitative understanding of the interfaces between each part. Consideration was given during this process if the input would be amplified by the following part or reduced. With a basic understanding of the incident, the identification of amplifiers appeared self-evident.

The size made it easy to get lost in the spreadsheet matrix. However, colouring the labels improved the understanding of where the enumerated number resides in the matrix.

The CAM-C diagram shows where the interfaces are and, just as importantly, where they do not exist, which aids understanding of the overall system.

In this particular CAM-C, it was found to be beneficial to differentiate between those causes that influenced the original event from those that impacted subsequent events.

Table 39 Baildon CAM-C

			Culvert		Pipes	Ballast	Sleepers	Drain	Train	Mtce Eng	MoM	signaller	Route controller							
			101 102	103	104	105	201	202	203	204	205	301	401	402	403	404	405	406	407	408
Culvert																				
	101 102	Blocked																		
	103	Structural collapse																		
	104	Water leaks out of manholes				3														
Pipes																				
	105	Flow not enough																		
Ballast																				
	201	Fallen away																		
	202	Washed away								1										
Sleepers																				
	203	Moved		2																
	204	Sleeper not supported				3	3													
Drainage																				
	205	Overwhelmed			2															
Train																				
	301	Derailment						3	3							2	3			
Mtce Eng																				
	401	Failure to spot fault																		2
MoM																				
	402	Failure to spot fault																		2
	403	Failure to spot fault no access																		
signaller																				
	404	Stop trains																		
	405	Stop trains wrong info										3	2							3
Route controller																				
	406	Stop trains																		
	407	Fail to give clear instruction																		
	408	Fail to interpret message correctly																		2

Key 3 – amplifier
2 – carrier
1 – resistor
-10 - terminator

post event mitigation

Tracing

As explained in Appendix J and Chapter 6 Section 6.3.4.3 risks can be traced using CAM-C through the system from the overall system level, in this case 301 'train' through the various subsystems to the root causal risks. This tracing process uses the causal failures on a row to identify the next subsystem or part ('level') to be traced. An example trace is shown in Table 40 using data from this CAM analysis of Baildon to illustrate the process.

Table 40 Example trace

Output	Input	Comment
301	204, 203	In this case, the sleepers have not moved. Instead, the ballast has gone. Therefore 204 is taken forward.
204	202, 201	In this case, it is known that the ballast has been washed away rather than fallen away. So, 202 is taken forward.
202	205	The drainage, capability of the track bed has been overwhelmed. However, there is a resistive effect because some water will drain through the track bed as a design feature.
205	104	The cause of this is water coming from the culvert which is fed by pipes.
104	105	The root cause is the pipes injecting a high-pressure, high-capacity flow.

There are no 'terminator' links in the CAM-C that will act to stop the overall failure effect. Even so, the drainage dissipates the effects of the flow of water from the culvert and is designated as a 'resistive' link, which is shown in Table

39 as a link from item 205 (the causal risk) to 202 (the output risk) with a '1' in the intersecting cell.

The sleeper failure 203 and 204 are both amplifying causal failures to the derailment risk 301, which is at the point of harm. It also appears that in turn there are amplifying links to 203 and 204. Therefore, the analysis indicates that the system is sensitive to these failures and it seems, the key subsystem appears to be the sleepers. If they move or are unsupported, there is a risk of a derailment due to unstable track. This causal trail leads back to either a structural collapse or flooding from an overflow of the culvert, as shown by the example trace in Table 40.

The rationalisation – Stage 4

Key points summary

Overall, the CAM-C indicates that the modelled Baildon railway system is a linear progression of flows through subsystems. Given the linearity the scope for rationalisation is limited because the relationships between subsystems are simple. However, there is some minor rationalisation that is undertaken.

Linkages

The population of the CAM-C is the point in the analysis where the analyst shapes the analysis to focus on those areas of interest. The Author judged from the information in Appendix D that items 101, 102 and 103 do not feature because although they pose a potential risk, they did not contribute to the potential incident which is the focal point of this analysis (as defined in the

CAM-ERD) and consequently are left blank indicating there is no link. Similarly, 201 did not feature in the information for Appendix D and is left blank, for this analysis. There is no link from 404 and is left blank because the lack of information occurred after the initial event to stop the first train. There is no opportunity to simplify the system analysis through terminator links because they are not present in this particular system.

Internally linked items

There are two links that are rationalised as an internal link, 403 to 402 and 407 to 408. Link 403 is a contributory factor to 402 the missed inspection. Likewise, 407 is concerned with the controller's impression that the incident was under control and is a form of confusion.

Summarisation

The rationalisation is taken further, 104 is taken as the summarisation of 105 and 104. These are the cause, with the source of the water plus the manhole design faults. Together these are regarded as a design cause. Item 204 could be argued to be a version of 203 because the sleepers are tied to the rails, as identified in Appendix D (fact 24). However, there could be movement in the sleepers as well as not being able to support the load, because they are mounted on ballast (Appendix D fact 25) and on that basis, it has been left in the analysis.

Commentary

There was not a great deal of simplification through this step. However, there was a small positive impact on the complexity of the analysis.

The rationalisation was simple where amplifiers were concerned. However, it was a subjective decision of where to undertake the summarisation. Similarly, the decision to retain items 203 and 204 required logical deduction of each part's role in the overall system. Using CAM-C as a tool helped with deductions because it allowed what-if questions to be posed.

CAM-Stage 5 Summarisation

Key points summary

The next stage of the process, Stage 5 in Figure 30, summarises and presents the results of the analysis; created by following the instructions in Appendix J. The information was selected from the CAM-C to show the failures that have an effect on the focus of the analysis as described by the CAM-ERD. This information allowed rows to be identified from the FMEAs, and combined into an overall FMEA.

The extracted CAM-C information was used to construct a combined FMEA, Table 41, using the risks identified as salient to the possible incident. Following the process described in Appendix J, the frequency was adjusted to account for the summarisation of 105 into 104 which took place in the rationalisation stage of CAM. The link between 105 and 104 is an amplifier, and the frequency

of 104 has been doubled from an occurrence of 20 years to 10 years, indicated in red to represent an equivalent risk.

Table 41 also contains two additional columns, the first, is an indicator of those failures that extend the time at risk after the first event of a train running on the unsupported track, but do not affect the initial incident. The second column has been constructed as shown in Appendix J. It is an indicator of the effect of the linkages in the CAM-C i.e., the balance of the number of amplifiers and resistors in a trace path between the output level risk and the failure being assessed. The failures are scaled with reference to the safety harm at the system level (risk 301) and each cause is traced through the CAM-C. Where an amplifier link is encountered, one is added to the count, and where a resistive link is encountered, one is deducted. For example, item 104 has two amplifiers in the path and one resistor, resulting in a count of one. While item 202 encounters two amplifier links resulting in a count of two. These counts are then used to adjust the frequency of occurrence of the failure.

The full combined FMEA is contained in Appendix G, which is taken forward to form the CAM analysis cause-consequence table. The resulting FMEA indicates two physical causes that cause the rails to fail to support the train. The analysis indicates that people interactions are more complex, reflecting that people are more flexible in an overall system and can be used to fill gaps in the physical design. The inputs from items 401 and 402 indicate that the Maintenance Engineer (Track Technician and Track Section manager) and Mobile Operations Manager have some parallel duties and could have interceded to identify that the track is not intact. Likewise, if they are incorrectly

directed on what to do, then they will fail as identified in the interaction with the Route Controller. Finally, the CAM-C indicates that all the key people had a chance of preventing the incident for following trains but not the initial incident with the first train. This is shown by the linkages for the physical failure not going through any of the people. In contrast those linkages for investigation and control all go through people-controlled risks in the CAM-C. These findings align well with the RAIB findings providing assurance that CAM is highlighting the correct things from the analysis, moreover there are additional risks found indicating a greater depth of analysis.

Table 41 Extract of the system-level FMEA table

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Secondary hazard	Increase at sys level
104	Culvert	Water volume flow	Failure during operation	Water flows out of inspection manholes	water flows down the embankment	High water flow along the railway	2	S	Pressure too high. Pipes contribute to pressure	20yrs 10yrs	Control of pressure and flow volume. Also, provide run-off drainage	Reports from the surrounding area and calculations	5		The pressure forces the water to rise up the inspection manholes and pop the covers. Note that there was a recommendation previously to divert the overflow into soak drainage. However, there is nothing which makes it an issue. Combined effect from 105		1
202	Ballast	Support sleepers	Failure during operation	Washed away	Sleepers unsupported	Possible derailment and injuries	4	C	Strong water flow	20yrs	Keep water in drains or fit retaining mesh to the ballast. Also, GE/RT8000-M3 stopping trains	Inspection and reports	3		If the sleepers are left in mid-air, a train will cause the rails to bend and possibly cause a train to overturn or derail. There is a rule book instruction to stop trains when there is a flood.		2

Table 42 Extract of the Cause-consequence table

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Consequence	Control	Evaluation type	Likelihood	Consequence	Risk
104	Manhole leak	High Water flow	Pipes	Pipes do not allow enough flow causing pressure rise and water to burst out of manhole covers and flows at a high rate	Water flows onto the railway	Railway track bed is flooded, and water is fast flowing washing out ballast causing a derailment as injuries	Injuries and possible fatalities	Design control of flow and pressure	Risk Estimation	Occasional	Catastrophic	Intolerable
202	Ballast removal	Track unstable	Ballast washed away	The ballast is not fixed and is washed away by a flow of water	The track is unsupported and becomes unstable. It is unable to support a train	Track moves and derails a train causing injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable

Following the method described in Appendix J for Stage 5, Appendix G analysis shows that the system-level FMEA is converted into a cause-consequence table that indicates the level of risk for each hazard by translating the FMEA occurrence and severity into risk levels using an EN50126 (CENELEC, 2017) risk matrix described in Section 7.1. Additionally, the frequency is adjusted by using the count from the 'increase at system level' column. It is used to amend the frequency by factors of two from the system level FMEA to those in the cause-consequence table below, when translated through the risk matrix of Section 7.1. An extract of this table is given in Table 42. It illustrates the effect of the amplifier on the system by raising the likelihood from 'Rare' to 'Occasional' for hazard 104.

Commentary

This stage converts the subsystem levels into the overall system levels. Initially, the multiplication factor was 10 for each 'level count' to create a logarithmic scale. However, it became clear that this was too high and effectively separated any adjustment into a highly amplified and attenuated group. There appeared to be no semi-linear scaling effect. After several attempts of trying values (5 and 1.5), the value of two seemed appropriate. It provided an effect that is noticeable but does not unduly distort the output and allows differentiation between the different number of 'level count' effects. This adjustment was fed back into the development.

7.3.6 Findings from study and lessons learned

Table 43 Comparison of findings

RAIB finding summary			New method (CAM) findings		
Ref	Primary causal factor	Secondary causal factor	Primary causal factor	Secondary causal factor	Commentary
1	Ballast under one rail washed out	<ul style="list-style-type: none"> d. Drainage could not cope with quantity of floodwater e. Flood water directed onto single sided embankment f. Previous flood repair did not withstand water flow 	<p>The wash out of ballast is identified in item 202, but it is not the root cause. The root cause is identified as the culvert through 104, which is the source of the flood.</p>	<ul style="list-style-type: none"> d. The drainage is identified as overwhelmed in 205 when it is fed with water identified in 104 e. The flood water flow is identified in 104 and 205 f. The ballast 202 and rails 204 indicate this is a risk. 	<p>The method has identified all the elements with the exception of 1f which is a comment on the adequacy of the previous repair. However, there is evidence from the analysis that the root cause is the design of the culvert which is not clearly identified in the report. First, the analysis shows that the hazard of derailment is created by physical changes, through the CAM-C. It is shown through the tracing of the risks from 301 to 204, 204 to 202, 202 to 205 and 205 to 105. Where 105 is the risk associated with the pipes which is part of the culvert design.</p>

RAIB finding summary			New method (CAM) findings		
Ref	Primary causal factor	Secondary causal factor	Primary causal factor	Secondary causal factor	Commentary
2	Reports of track damage not dealt with appropriately	<ul style="list-style-type: none"> e. Controllers did not listen carefully to emergency calls f. Controllers misdirected responders to a different location g. Responders not aware of the vulnerability of embankment to flooding h. A third train was allowed to traverse the washed-out track section when the line was blocked 	The adequacy of dealing with reports and passing information is identified in 408. However, what appears to be more crucial is the misinformation provided to the signaller (405), although this is later shown to be an intermediate level risk.	<ul style="list-style-type: none"> e. The confusion of the controllers is identified in 408 f. The misdirection is highlighted in 408 g. This item was not identified. However, this was not evident from the extracted facts. h. The routing of trains in error is identified in item 405 	All bar one of the elements has been identified through the method. Item g was not evident from the identified facts in Appendix D. Furthermore, the analysis shows that the signaller is the key actor, and he was misinformed. The analysis shows that the people-based risks were secondary effect.

In summary, the CAM process has been followed as set out in Appendix J and illustrated in Figure 30. A set of incident 'facts', Appendix D, has been used to standardise the input to the process. It appears the new method has been effective in identifying similar findings to those in the official RAIB report. If CAM was deficient as an analysis tool, findings would have been missed. Also, the root causes appear to have been identified; the success criteria have been met and exceeded by highlighting the root cause rather than pointing to the symptoms. The Author has no comment on the RAIB process only that from the evidence CAM appears to have done better.

From this analysis, the permanent solution appears to be to redesign the culvert system to lower the pressure under the railway and avert the flow of water across the tracks. Alternatively, the railway drainage could divert the excess water, but this would just treat the symptom rather than the cause.

One of the findings concerning people (item g) was not identified. An inspection of the facts in Appendix D shows that this was not in the evidence, therefore the analysis cannot be reasonably expected to identify it.

7.3.6.1 Feedback and improvements to CAM

1. A key step where guidance to practitioners is required is the factor to be applied to amplified hazards. This was fed back into the process and now forms an improved Stage 5 of CAM, as described in Appendix J.
2. Additionally, the utilisation of the CAM-ERD and CAM-C enabled the Author to identify the salient hazards from the failure data in the FMEA. This

feedback has been incorporated into CAM and it is described as part of Stage 5 in Appendix J.

Furthermore, it was noted because the Baildon modelled system was effectively a linear progression of subsystems there was limited opportunity to employ rationalisation techniques in CAM-C to create a simplified version of the summarised risk analysis. However, as explained in Appendix J and illustrated in the following paragraphs, rationalisation can be employed to identify the 'true' root causes by eliminating intermediate links.

Finally, the management summary risk matrix reproduced in Table 44 illustrates the effect of simplification inherent in CAM and points to the culvert as an intolerable risk (104). The secondary risk of 'confusion' (408) is also highlighted as an intolerable key risk. As, indicated by RAIB this 'confusion' is a symptom of a lack of clear processes and responsibility. The presence of a large number of risks in the 'catastrophic' column of the matrix and greater than an improbable likelihood of occurring is, in the Author's experience, symptomatic of a system that is out of control.

Typically, when examining a system, a distribution of risks would be expected to some extent across the likelihood/ consequence spectrum. However, in this case, that characteristic is absent. Instead, the absence is likely a characteristic of the RAIB source data being 'cleansed' of those factors that are not at high risk to create a focused message about the incident.

Table 44 Baildon risk matrix extracted from Appendix G

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					
Probable					
Occasional					104, 408
Rare					202, 203, 204, 205, 401, 402, 406,
Improbable					405
Highly Improbable					301

CAM-C has been used to differentiate secondary and primary risks. Primary risks in this case are those that would have prevented the initial physical event happening if they had been addressed; while secondary risks are those that affect the post event outcomes. Those risks that arose after the initial event were coloured beige in the CAM-C. These were identified from the ‘facts’ in Appendix D. In particular, the people risks are determined to be secondary because their intervention only occurred after the initial event. Therefore, there are six primary risks (104, 202, 203, 204, 205), all these are physical, and one is intolerable (104). This outcome suggests that the recommendations from the official report should have placed greater emphasis on the physical short comings rather than the people. From a CAM process perspective this differentiation shows the flexibility of CAM-C.

The analysis identified the key hazards as:

Table 45 Hazards from CAM analysis

Ref	Hazard	Description
H1	High Water flow	Flow from the culvert manholes provides the source of the high volume of water that triggers that incident.
H2	Track unstable	Ballast not supporting the track. The track is not properly supported and likely to move.
H3	Track in poor condition	Rail bends under load which could cause a train to derail
H4	Track fault undetected	Track fault undetected is left in place.
H5	Line open	Damaged line open to traffic
H6	Control actions ineffective	Key information is not understood or discarded which is effectively lost to the control process this leads to delays in action or incorrect action.

Table 46 shows the hazards from the analysis after this a further rationalisation process has taken place, as explained in Section 7.3.5. There are three physical

system hazards (H1-H3), indicating a focused incident interface concerned with track condition and water flow; while, in contrast the hazards the people pose (H4-H6) are more varied, reflecting their different roles.

Further rationalisation can be applied to remove the intermediate risks as described in Appendix J for Stage 4. The trace technique is used to find the root causal risks and to remove the intermediate risks. However, it is applied later in the process in this case to emphasise the value of this part of CAM. When this is applied there are three risks left as the root causal risks (104, 406 and 408) that describe the incident risks.

Table 46 Baildon rationalised risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent	Yellow	Red	Red	Red	Red
Probable	Yellow	Yellow	Red	Red	Red
Occasional	Yellow	Yellow	Yellow	Yellow	Red (104, 408)
Rare	Green	Green	Yellow	Yellow	Yellow (406)
Improbable	Green	Green	Green	Yellow	Yellow
Highly Improbable	Green	Green	Green	Yellow	Yellow

As can be seen from Table 46, that there are just three root causes for the risks. This simplification is powerful.

7.3.7 Research success criteria satisfaction

In Chapter 1 three criteria were set to gauge the success of CAM. The table below summarises how these were fulfilled in this case study and the extent to which the criteria were achieved.

Table 47 Test case success measure

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
Economic	<ul style="list-style-type: none"> An efficient method of performing the analysis. No high-powered computers or software packages required. Time to complete is less than 5 days. Analysis pages to be less than 50. 	<ul style="list-style-type: none"> The test case has demonstrated an analysis without specialised computing support. It has shown that the salient subsystems and their relationships were identified. The analysis quickly focused on the critical relationships. No complicated maths was required. The duration of the analysis was within the time limit. 	<p>Estimated analysis time</p> <p>Approximate number of analysis pages</p>	Yes	Yes	2 days 25	Successful

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
Applicability	<ul style="list-style-type: none"> Applicable to railway engineering safety risk assessment problems with single and multiple systems. 	<ul style="list-style-type: none"> The successful identification of the risks with the Baildon test case has demonstrated that CAM can be used with multiple separate systems that include physical features and people as evidenced by the CAM-ERD. 					Successful

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
Safety	<ul style="list-style-type: none"> As a minimum the same hazards and or causes are identified as the findings in the official report 	<ul style="list-style-type: none"> The test case analysis has identified the causes originally reported, except the single secondary cause where there was no evidence, as described in Table 43. A different primary cause was identified for both the initial event and secondary events. The rationalised matrix, Table 46, points to the critical cause of the incident, item 104, which was missed by RAIB. The rationalisation stage in CAM is powerful because it eliminates the less important risks from the analysis summary. 	<p>Number risks identified</p> <p>Number of risks missed</p> <p>Number of additional hazards identified</p>	<p>Yes</p> <p>Yes</p> <p>Yes</p>		<p>6</p> <p>1</p> <p>1</p>	Surpassed expectations

7.4 Comparison of CAM with other methods

Previously CAM has been compared with the RAIB investigation and shown to produce acceptable results. This section goes on to compare CAM with several other analysis methods used in the rail industry and gain a relative estimation of how CAM performs. The same reference incident data as was used in the previous section is reused to provide a consistent reference for the comparison.

The Baildon incident has been analysed using three methods, CAM, STAMP and Yellow Book (YB) to provide a basis for comparison, using the 'success criteria', Table 2, in Chapter 1 Section 1.9.1. In each case the analysis was carried out by following the methods published in their respective documentation (Leveson and Thomas, 2018a), (Rail Safety and Standards Board, 2007) and Chapter 6 of this thesis. Each method was used in a forward mode to generate the hazards and estimate of the magnitude of risk, where possible, from the source documentation. As can be seen from the vignettes in Table 48, the proposed techniques have different characteristics; this is expected as a similar observation was made for the current risk analysis technique assessments in Chapter 4. There is a common link between CAM and YB, because CAM draws on some of the same analysis techniques for the Stage 2 subsystem analysis as YB uses.

Table 48 Risk analysis technique vignettes

CAM	YB	STAMP
<p>This is a 5-stage process that is dedicated to safety risk analysis. It analyses the subsystems and creates an overall system risk view.</p>	<p>This is a 7-stage process that incorporates traditional analysis techniques at each stage of an overall analysis process.</p> <p>The process is designed to take the analyst from identification through to a loss analysis and justification of the outcome. As a result, the scope wider than a safety risk analysis.</p> <p>For equivalence with the other processes only stages 1 (identification), 2 (causal analysis) and 7 (acceptability) are required for this analysis</p>	<p>This is a system based multistage process that consists of 4 stages: purpose of analysis, model of system, identify unsafe control actions and safety limitations, and describe possible accident scenarios.</p> <p>The process does not directly identify the causes but they can be deduced from the output.</p>

A variant of STAMP, System Theoretic Process Analysis (STPA) was chosen as representative of the modern sociotechnical methods, and although not popular in the Chapter 4 industry survey with less than 20% using it, it has been cited (Underwood and Waterson, 2013b) as a possible technique. Yellow Book (YB) was chosen because it has been established as a safety analysis manual for a number of years within the rail industry and can be thought of as representing the traditional approach to risk analysis, as indicated by Dunsford and Chatzimichailidou (2020), an FMEA/FMECA tool was selected as representative from those cited in YB because it is the most popular method, as indicated in Chapter 4 with a score of over 60%.

All of the analyses used Appendix D as the source data. The data was used in lieu of a hazard identification workshop. The analyses are contained in:

Table 49 Analysis index for methods

Method	Analysis appendix
CAM	Appendix G
STAMP STPA	Appendix H
Yellow Book	Appendix I

7.4.1 Commentary and discussion

The analysis was carried out on incident data and there was no attempt to cost solutions and mitigations. The objective was to generate a set of hazards and causes in each case. As a result, the YB seven stage process was only partially implemented, as indicated in Table 48 to make certain the three risk analysis methods CAM, YB, and STAMP had a similar scope.

It is apparent STPA is a very different approach to the traditional ways. It starts with an accident or loss and strictly defines the system level hazards as those

states that would under severe conditions lead to an accident or loss that has been nominated at the beginning. At this point in the STPA process there is no equivalent of the unrestrained hazard identification process, because it is concerned with identifying loss and associating system level hazards with this loss. This has the effect of limiting the number of identified hazards, shown in Table 50, in this case to three. In contrast CAM initially identifies 16 candidate potential hazards later reduced through the CAM process to six significant hazards, as shown in Table 51, at the system level and YB indicates there are 12 throughout. For YB and CAM the hazard identification process implies a divergent strategy, such as brainstorming and CAM-ERD, to capture as many possibilities as is reasonable.

Table 50 Initial hazard identification stage hazard types

Process	Hazard type			Comment
	Physical	Process	Sub	
YB	5	7	0	Failure modes were used as a surrogate.
STPA	2	1	2	The sub-hazards are specialisations of the main physical hazards
CAM	10	6	0	Failure modes were used as a surrogate at this stage, because of the selection of the subsystem analysis tool.

Table 51 indicates the hazards found after the three risk analyses have taken place.

Table 51 post analysis significant hazards identified

Process	Hazard type			Comment
	Physical	Process	Other	
YB	5	7	0	The particular method chosen FMECA does not directly lend itself to hazard identification. In this case the failure mode has been taken as a surrogate for a hazard in line with (Lepmets, 2017)
STPA	2	1	2	The two others are sub- hazards which are specialisations of the main hazards
CAM	4	2	0	

Table 52 shows the number of causes that were identified by each of the three risk analysis methods. It is striking that STPA has identified significantly more causes than the other risk assessment methods. It seems to suggest that the STPA process is a divergent process which produces a large number of causes relative to the number of hazards identified. This phenomenon is probably a side effect of the last two stages in the STPA process, described by Leveson and Thomas

(2018b), where unsafe actions are brainstormed from the control model and various scenario sentences are constructed from these actions. For this analysis the causes were, as an additional step, extracted from these scenario sentences. This expansion of information is clear from an inspection of Appendix H where the control actions and scenario sentences cover many pages.

A weakness of STPA, is the scenarios are subject to the analyst’s imagination and can be seen as a discriminator on the quality of the analysis. Although, it is clear that the corresponding weakness in CAM and YB is the imagination applied to the hazard identification process. STPA identified a total of 120 non-unique causes of which 91 had no identifiable facts from Appendix D to support the assertions. By contrast CAM uses only the 18 risks and YB 12 all were supported by the facts from Appendix D. It indicates that brainstorming approach in the last two stages of STPA induces a ‘scatter gun’ approach to the problem, whereas the other methods align the causes to the facts in the identification phase. The 29 causes identified by STPA are nearly all process based with only 3 physically based causes, this is an effect of the emphasis of STPA and STAMP on processes and hierarchies as shown in the Chapter 4 current methods analysis and noted in the literature review of Chapter 2.

Table 52 Post analysis cause types

Process	Cause type	
	Physical	Process
YB	5	7
STPA	3	26
CAM	6	5

As can be seen from Table 52, both YB and CAM there is a greater emphasis on the physical causes. Additionally, it is clear from the CAM analysis reported in Section 7.3.6 due to the linkage descriptions in the CAM-C that the process causes are associated with the secondary effects, which is not clear from the other analyses because there is no equivalent matrix. When the full rationalisation is applied in CAM by removing intermediate links, as demonstrated by Table 46, the number of causes reduce to three key items.

To clarify whether an analysis method relied on physical or process facts of the Baildon incident, the Author classified each fact in Appendix D. An analysis was conducted by the Author to identify which fact was identified with each risk for each of the three analyses using an Excel spreadsheet matrix. Cells were marked with a 'Y' and a red background to indicate that the fact was used, and associated to a particular risk. Figure 32 shows the use of facts from Appendix D in each of the analyses. Each fact was classified as either a physical fact or a process fact and ordered to show physical facts at the top and process facts at the bottom. As can be seen both YB and CAM use a mixture of physical and process facts, while STPA aligns with purely process facts, which may explain the bias toward process explanations with STPA.

Visually comparing the coverage shown in Figure 32 indicates that CAM provides a richer picture of the incident because there are more ‘Y’s, indicating that YB analysis may produce a more superficial outcome. The initial impression is confirmed from the analysis in Table 53.

Table 53 Analysis density ratios

Method	No of Ys	No Hazards	Density ratio
CAM	45	19	2.4
YB	26	12	2.2
STPA	38	31	1.2

As indicated in the table CAM has the highest fact/hazard density ratio as well as over 50% more individual hazards. Furthermore, it is clear that STPA performs poorly on this metric.

Both CAM and STPA make use of the system structure. CAM uses the CAM-ERD to depict the system structure, as an aid, while STPA uses a formal control structure as part of the second stage of analysis. The STPA control structure is restricted to functional control links because of the strict process rules. This restriction has led to a greater focus on lines of authority and hierarchy of socio control rather than the CAM approach which manages to capture both the socio and physical linkages for further analysis in the CAM-ERD. CAM allows the CAM-

ERD to be constructed by including various relationships between the parts, encouraging a rich picture. An advantage of the CAM-ERD over the STPA control diagram is the identification of the points of harm within the diagram which help focus the analysis.

From the STPA process description by Leveson and Thomas (2018b) it is easy to see how the physical components of the system are given a much lower weight in STPA with them being designated as contained in a controlled process, this is borne out by the analysis in Appendix H. The CAM-ERD provides divergence and categorisation of elements into subsystems at the start of the process which appears to have a positive impact on the flow of the risk analysis. Whereas CAM and YB identify the drainage and culvert as key components STPA struggles, with the component left until a final 'catch all' scenarios part of the process as shown in Appendix H.

In comparison with the other methods YB is initially concerned with designating the system boundary without being concerned about how the system is constructed. This approach misses an opportunity to gain an understanding of the system parts before proceeding with identification. It relies on the identification process identifying the key features for analysis, in this case an FMEA is used, although other 'creative' methods could have been used such as HazOP.

Although FMEA is used in both CAM and YB, there is no equivalent scene setting of the CAM-ERD in YB, therefore the detail is not available to populate the FMEA in detail and very much relies on the analyst to brainstorm risk spontaneously.

Therefore, this is a limiting part of the YB process and the quality of the analysis.

In contrast, CAM has an identification process CAM-ERD for each subsystem

within the system boundary and where necessary interfacing subsystems outside the system boundary. Consequently, the CAM method leads to a richer list of potential hazards and causes because there are prompts in the CAM-ERD to drive the analysis. Furthermore, YB does not have a defined process for combining subsystem analyses into a whole, instead it is left to the analyst's skill. In contrast, CAM supports the integration through the CAM-C process, reducing cognitive complexity as described at the end of Chapter 2 Section 2.3.

Finally, a comparison is provided of whether the various risk assessment methods identify the causes cited in the official report (Rail Accident Investigation Branch, 2017). Table 54 has been constructed from the results of the three analysis methods, which are detailed in Appendices G-I. Where a cause has been identified in the analysis matching a finding from the RAIB report findings a 'Yes' is inserted into the table, similarly where the analysis failed to identify a RAIB finding a 'No' is inserted. It is clear from Table 54 that CAM has the overall better coverage.

Table 54 Comparison of analysis findings against the official report (Rail Accident Investigation Branch, 2017)

Process	Primary causes		Secondary causes						
	Ballast under one rail washed out	Reports of track damage not dealt with appropriately	Drainage could not cope with quantity of flood water	Flood water directed onto single sided embankment	Previous flood repair did not withstand water flow	Controllers did not listen carefully to emergency calls	Controllers misdirected responders to a different location	Responders not aware of the vulnerability of embankment to	A third train was allowed to traverse the washed-out track section when the line
CAM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
STPA	Yes	Yes	Yes	No	Yes	Yes	Yes	No	*
YB	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes

The ‘*’ indicates that the analysis is not specific about the order of events and does not point to an additional train.

From a review of the YB analysis in Appendix I, in the Author’s opinion, the failure to identify the drainage finding (third column), is probably due to the identification stage. In this analysis the system to be examined is identified as a single entity, unlike CAM which uses the CAM-ERD which decomposes the system into subsystems. In the case STPA it seems to the Author, from a review of Appendix H that the failure to identify the flood water cause (fourth column) is due to the concentration on control actions and people rather than the physical aspects of the incident. The ‘No’s in the eighth cause column for all the methods is due to a lack of evidence in the factual statements of Appendix D.

Table 55 Estimated elapsed analysis time and page count

Process	Estimated elapsed analysis time (Days)	Approximate appendix page count
CAM	2	25
STPA	6	61
YB	1	17

Table 55 shows the estimated elapsed analysis time noted by the Author for each of the analyses. This is a rough estimate due to distractions and interruptions during the analyses, nevertheless it provides an indication of the relative efficiency of the methods. As can be seen STPA took considerably longer than the other methods. In the Authors opinion this is probably due to the large amount of information that needed to be processed. YB is the shortest and probably reflects that the analysis is not as in depth as CAM due to the identification phase. CAM and YB are both within the efficiency target set for CAM of 5 days in Table 35.

The elapsed time comments correlate with the physical size in page numbers of the analyses as shown in Table 55. Assuming the number of pages equates to analysis effort, it indicates that relative to a CAM analysis YB analysis takes 68% of the effort while and STPA takes 244%.

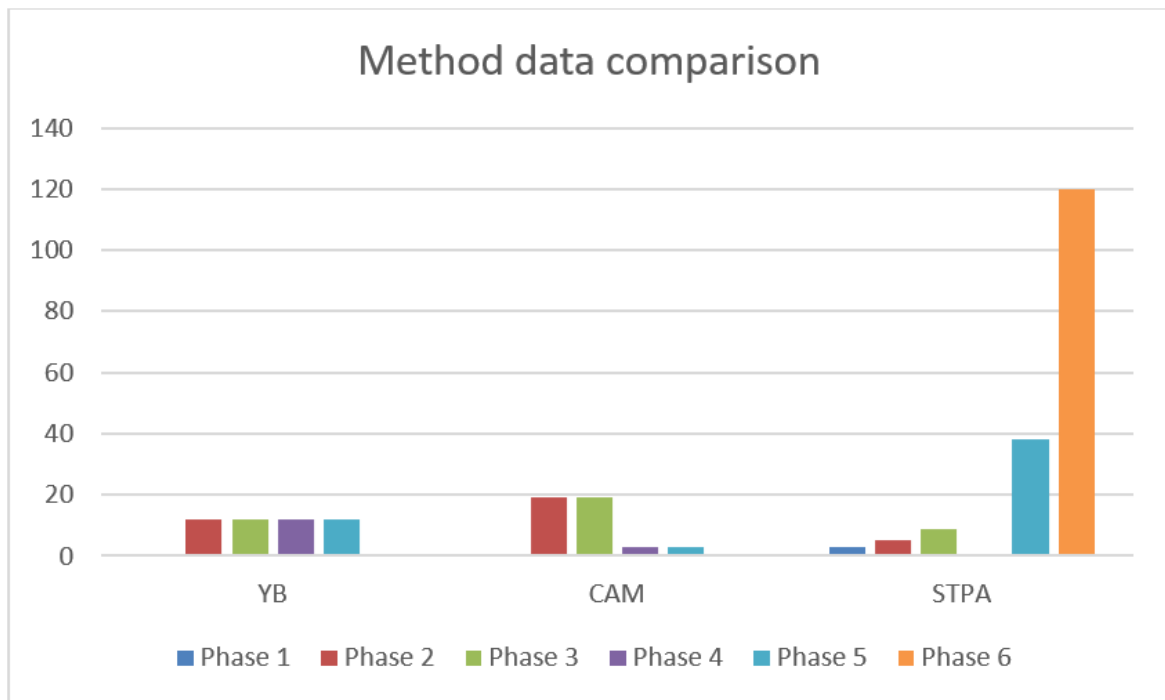
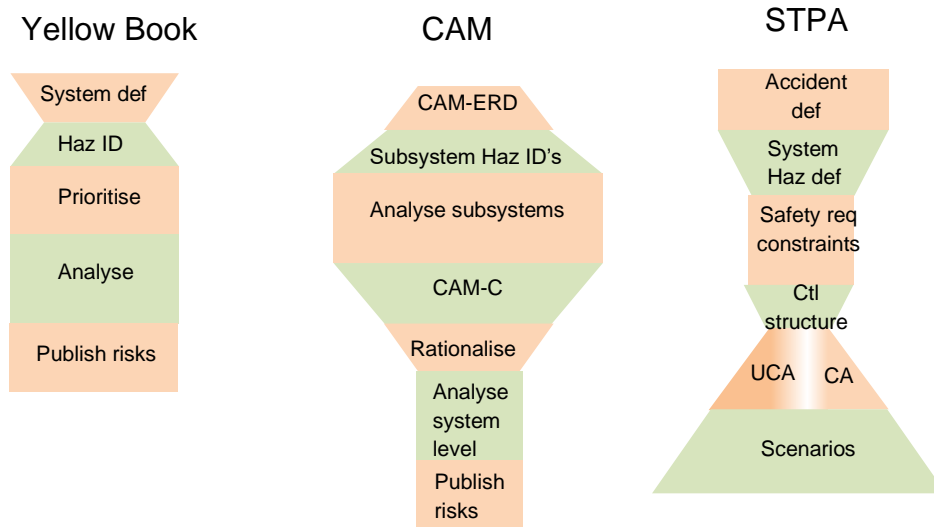


Figure 33 Risk assessments data usage

A further indication of effort and focus of the analysis is obtained by looking at the data usage for each phase of the process. The term phase is a generic term used for this assessment and stands for the part of the process undertaken, it avoids confusion with any specific assessment method 'stage'. It is the volume of data that is of interest rather than the specific activity in the phase. Figure 33 has been constructed by counting the data rows of the matrices in Appendices G-I. In phase 1 of the YB and CAM and phase 4 of STPA there are no matrix rows as these use diagrams and other means to express the information, hence they are left blank. As can be seen there is a large expansion of data in the STPA; while the data is constant in the YB case and the data is reduced towards the end in the CAM process. A conceptual visualisation of the data spread is shown in Figure 34.

Figure 34 Conceptual depiction of data space



7.5 Summary and conclusions

The case study has been undertaken in two parts, first a test case application of CAM has been performed and it has been shown that the analysis has correctly identified the findings from the official incident report. Moreover, CAM has provided a number of insights into the incident that were not apparent in the official report. In particular the design of the culvert has been identified as the root cause of the incident and that the ‘people’ related activities only affect the time at risk after the initial incident. The capability of the method to simplify the analysis output appears to be of value because the critical risk causes are highlighted.

The second part of the case study has compared the performance of CAM with STPA, a STAMP derivative, and Yellow Book, which represent the new sociotechnical and traditional approaches. Steps have been taken to reduce research bias through the adherence to written processes in each case. The comparison has shown that CAM has a superior performance in several areas,

subsystem and cause identification, hazard identification, integration into a whole system analysis and rationalisation of the output. The comparison suggests that CAM is a viable analysis method that focuses on the key parts of the system under consideration.

Figure 34 shows a conceptual coverage to the analysis data space for each of the three analysis systems. It has been created from the comments in Section 7.4 on the analysis, principally from Table 55, using the number of items at each stage of the analysis to indicate how much data is being considered in that stage. It is striking that CAM is an expansive method at the beginning and reduces at the end of the process; whereas the other techniques to an extent are reduction techniques at the beginning. YB does expand the space after the initial process, while STPA reduces the space until the final stages. Comparatively, it seems that the CAM process has an advantage by providing the richest data set to work with and then extracts the salient items from it; whereas with the other techniques there is a greater chance that key items are missed as indicated by Table 54, which shows that CAM has identified all the causes, bar one.

Overall, the evidence shows that CAM has performed the best of the techniques in the comparative test case in respect of:

- It has identified the most risk causes;
- The efficiency has met the time limit;
- The effort required is not out of step with the YB method (which required the least effort);

- At each stage the method was subjectively understandable to the Author;
- It has been the most effective at identifying the most causes of the techniques tested.

In addition, CAM has satisfied the test criteria to validate the assertion that CAM is a useful risk analysis method¹⁸.

There have been learning points from the case study which are described in Section 7.3.6.1 as:

- Amplification factor guidance;
- Extraction of risks using CAM-ERD and CAM-C.

These have been incorporated into the method by altering Chapter 6 and Appendix J. Consequently, the method is now more robust.

¹⁸ All the other methods performed worse against the criteria by virtue of not identifying as many of the causes as CAM. Also, STPA needed a supplementary process to obtain the list of causes, which would have reduced its score on the applicability criterion.

8 Rail based application test cases and benchmarking of CAM

This chapter consists of two test case applications that are used to validate that CAM can be successfully applied to railway risk assessment problems of different types and to use one of the applications as a benchmark.

This chapter uses the updated version of CAM incorporating the lessons learned from Chapter 7.

The benchmark measures CAM against parameters derived by Underwood and Waterson (2013b) to gauge the suitability of as an analysis tool.

The chosen test cases are as follows:

Table 56 Incident selection criteria

Incident	Reason for selection
<ul style="list-style-type: none"> Grayrigg 	<p>This was the last major GB rail accident on the mainline that involved loss of life¹⁹. Having been studied by others it also provides a basis for a benchmark.</p>
<ul style="list-style-type: none"> Hong Kong metro - MTR Tsuen Wan Line 	<p>An accident on the Hong Kong metro involving the commissioning of a novel signalling system, which at the time of the analysis was a current issue. The requirements are slightly different because of the requirement to provide an indication of when it would be acceptably safe to recommence testing.</p>

The first test case is Grayrigg is used as a validation of CAM by comparing the results with the official accident report (Rail Accident Investigation Branch, 2011) which has been shown in chapter 7 to be a reliable reference. Grayrigg (sometimes referred to as Lambrigg) has been chosen because it was the last major accident where life was lost on the GB network, with the exception of the very recent Carmont accident (Rail Accident Investigation Branch, 2020), it has been used as a benchmarking case study previously by (Underwood and Waterson, 2013b). The analysis is undertaken in two parts. First, CAM is applied by the Author to the Grayrigg test case and the results of the analysis are

¹⁹ Loss of life has since occurred in a rail accident at Carmont near Aberdeen in August 2020.

compared with those obtained from the official RAIB accident report (Rail Accident Investigation Branch, 2011). Second, CAM is compared by the Author to the parameters described by Underwood and Waterson (2013b) to measure its suitability. Accimap, STAMP and SCM were scored in the paper by Underwood and Waterson (2013b) which also used Grayrigg data and comparisons can therefore be drawn with CAM.

The second test case is the Hong Kong Tsuen Wan Line study serves two purposes, it provides a demonstration of an application on a different type of railway (metro), and demonstrates CAM in the reverse mode because the analysis is undertaken by working in reverse from the accident.

8.1 Assessment of risk

These test case studies use a semi-qualitative method of assessing and evaluating the acceptability of risk derived from EN50126 (CENELEC, 2017), which is described in Chapter 7 Section 7.1. The Author has judged that this calibration of the matrix in Chapter 7 is suitable for use in these test case studies because the type of system is similar.

8.2 Grayrigg test case

The limitations on the RAIB accident source data are the same as those described in Chapter 7. As with the Baildon test case the Author has reason to have confidence in the findings of the RAIB report for the reasons described in Chapter 7 Section 7.2.

The source information used for this application test case of CAM is taken from the RAIB accident report (Rail Accident Investigation Branch, 2011) into Grayrigg.

The report has been used as the source of information for the case study and it provides a reference to compare with the CAM findings and validate CAM.

This was a significant accident on the mainline GB railway during 2007, where a fatality occurred due to a derailment. The accident is referred to as Grayrigg, however the points concerned are at Lambrigg, hence the accident is sometimes referred to by industry workers as the 'Lambrigg incident' which sometimes leads to the impression by the public that they are two separate accidents. The accident concerned the maintenance and fitness for purpose of a set of points on the West Coast Mainline (WCML) that caused a high-speed train to derail. Setting aside the terrible consequences, the accident has been recognised as significant not only because a RAIB report has been produced but also the accident has been used to benchmark other techniques as reported by Underwood and Waterson (2013b).

8.2.1 Test case success criteria

The measures of success for a case study were defined in Chapter 1 Section 1.9 as Safety, Economic and Applicability, which for this case are interpreted as shown in Table 57.

Table 57 Success measure interpretation

Measure	Interpretation
Safety	The CAM analysis outcome should at least include the same 'answer' as the official report, and if there are other factors, it should identify these too.
Economic	The process should be understandable and relatively effortless to implement without resort to specialist tools, such as specialist software packages or high-powered computers. Also, it should be possible to complete the analysis with a reasonable timeframe; within 5 days. Furthermore, the length of the analysis should within 50 pages.
Applicability	The process should be directly applicable to the railway environment without additional adaption.

The safety measure is factual, the economic is a mixture of factual and subjective while the latter measure of applicability is subjective. Subjective measures are demonstrated through illustration and success is judged subjectively by the Author.

8.2.2 Brief accident summary from the RAIB report

A full summary description of the accident particulars is provided in Appendix E.

This section describes the key points.

A Virgin Pendolino train consisting of 9 cars and travelling at 95 mph was derailed at Lambrigg 2B facing points, which were an emergency crossover. Eight of the cars came to rest at the bottom of an embankment with five overturned. One person suffered a fatal injury and many others were injured. Stretcher bar and out of tolerance adjustment failures left the switch rail free to move on the failed points causing the derailment by allowing the wheels to pass on the wrong side of the rails.

8.2.3 Analysis

The CAM analysis undertaken by the Author is fully described in Appendix E, this section contains summarised key points and commentary to illustrate the application of CAM and its features.

The Author has used CAM-FN (Forward New/novel/modified analysis) as explained in Chapter 6, Section 6.3.4. The process is reproduced in Figure 35 for convenience and the user instructions can be found in Appendix J. The Author has decided for the purposes of this test case that the CAM-FN variant is more appropriate than the accident variants because the objective is to see if a CAM analysis produces a set of outputs to be compared with the official report rather than attempt to trace the causes from an incident.

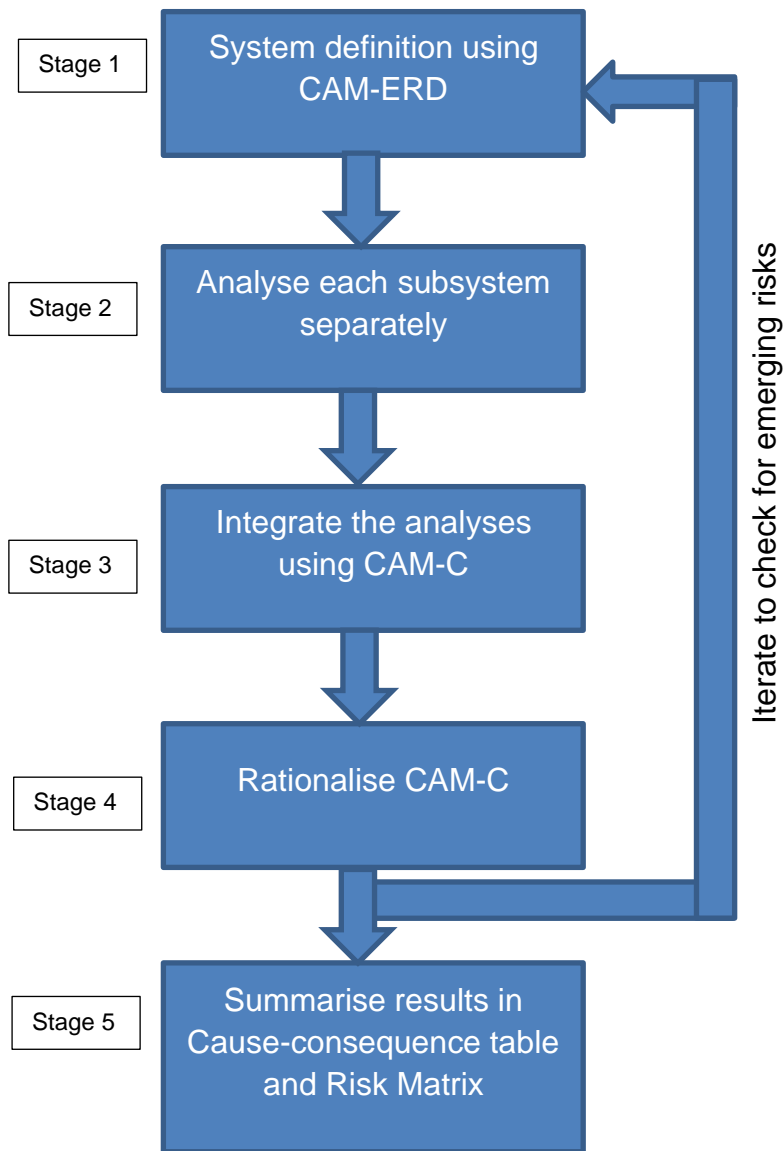


Figure 35 CAM_FN process reproduced from Chapter 6

The steps to carry out each of the stages listed in Figure 35 is described in Appendix J. The boxed ‘Stage’ labels in Figure 35 indicate the stage of the process. These are used in this analysis as bold underlined headers to indicate the process stage being described.

For this analysis FMEA has been selected as the method for the subsystem analysis because it was found to be the most popular from the industry analysis in Chapter 4.

CAM-Stage 1

Key points summary

The decomposition of the system has been accomplished via a CAM-ERD system into structural subsystems and behaviour flow is described in Appendix E.

The resulting CAM-ERD is shown in Figure 36. The major subsystems are indicated by circles while the parts are indicated by rectangles. The point of harm is indicated by a red triangle. Relationships are shown as arrows. As can be seen the interrelationships are clearly identified. There are some complex relationships between the process, points and maintenance. Clearly, harm is the result of the vehicle coming off the track, as shown by the triangle. The official report stated there was no fault with the train and it is treated as a combined system with multiple inputs for this analysis, as it appears to be the most sensible classification to focus the analysis on the infrastructure.

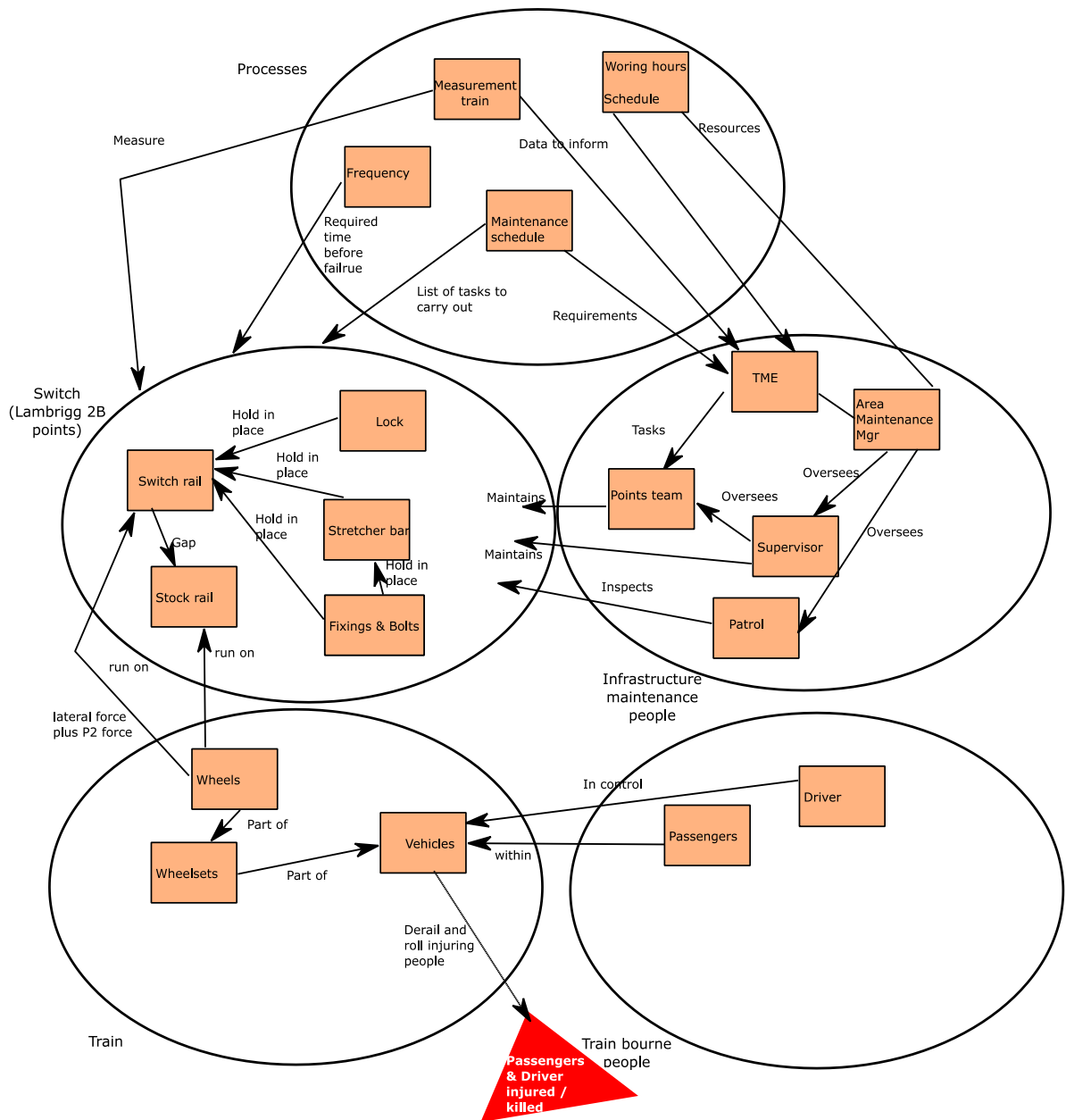


Figure 36 CAM-ERD diagram from Appendix E

Five subsystems have been identified. Each subsystem has a FMEA created for it as shown in Appendix E.

Commentary

The division into subsystems was straightforward because it followed the normal subsystems found on a railway.

Some of the process outputs appeared to affect all the parts of the switch system, and it was easier to link the processes to the switch subsystem and declutter the diagram. It was a similar case for the maintenance team.

The maintenance team subsystem parts relationships were difficult to fathom with what appeared to be multiple lines of authority, and there were multiple attempts at the diagram before rationalising the relationships.

The official report indicated that the train was not to blame for the accident and provided the opportunity to simplify the vehicle subsystem to model the interfaces.

The resulting diagram clearly illustrates where the interfaces and interactions are and provides a firm basis for subsystem analysis.

CAM-Stage 2

Key points summary

Each subsystem has been analysed using an FMEA, these have been created using EN60821 (CENELEC, 2006) and Anleitner (2010). CAM-ERD indicates that the maintenance schedule is a key parameter because it drives the other maintenance activities and the schedules feature throughout the FMEAs. There has been some manipulation of the FMEAs to account for the lack of implementation of the controls. This has resulted in an increased occurrence rate because the integrity of the physical components relies on regular maintenance controls.

Commentary

The FMEAs provide a summarisation of the failures in each of the subsystems. The adjustment of the occurrence rate required some judgement and background reading to understand why switches potentially deteriorate without regular maintenance. Once that was understood, an estimated factor could be used to adjust the occurrence rate.

8.2.3.1 CAM-C and cause-consequence

Key points summary

The CAM-C, Table 58, has been reproduced from Appendix E. Failures are used in this section rather than hazards because Stage 2 used FMEAs. The causes are listed in the columns and the resulting failures in rows. This is interpreted as described in Appendix J, the columns acting as causes for the failures indicated in the rows. Using the CAM-C, a chain of events can be traced through the system, using the process described in Appendix J Section J2. The individual entries can be traced back to the FMEAs through the 'Ref' entry e.g., 101. The resulting matrix is much larger than the previous applications, which reflects a more complex system. However, it is clear from the CAM-C that the main interaction is between the processes (in the 500 range) and the point components, because of the cluster of links in the top righthand corner of Table 58. Only a few of the people activities (in the 400 range) affect the points. The CAM-C seems to bring clarity to the interactions and where the key links are.

Commentary

The diagram construction was reasonably straightforward, using the CAM-ERD as a guide. The straightforward interfaces from the CAM-ERD appeared to make the task easier and justified the effort invested in getting the CAM-ERD right. The data points were extracted from the FMEAs with the CAM-ERD used to help understand the path and estimated using the CAM-C rules. The link values were adjusted several times to reflect an increased understanding of the importance of the relationships.

The CAM-C pictorially shows the centre of the interfaces as a process-centred system, helping to increase the understanding of the overall system.

Table 58 CAM-C reproduced from Appendix E

		Ref		101	102	103	104	105	106	201	202	203	204	301	401	402	403	404	501	502	503	504	505	
Switch	Stretcher bar																							
		101	Snaps			3			2															
		102	Loose			3													2	2	2	2	3	
	Joints																							
		103	Parts separate														3	3	2	2	2	2	3	3
	Stock rail																	2						
		104	Moves																					
	Switch rail																							
		105	Moves undertrain	2	2															2	2	2		3
	106	Gap too big														2	3		2	2	2	3	3	
Train system	Wheel																							
		201	Climb rail					3	3															
		202	Climb rail																					
	Wheel set																							
		203	Frame or suspension components break							2														
	Vehicle																							
	204	Structure buckles							2															
Train people	Driver																							
		301	Overspeed																					
People system	Area Mgr																							
		401	Schedule too much work																	3				
	Points team																							
		402	Task not carried out													2								
	Supervisor																							

CAM-Stage 4 Rationalisation

Key points summary

Given the concentration of the links there appears to be no call for rationalisation to be generally applied, other than to treat the train system as a single system level entity in the analysis going forward. Moreover, the extent of the rationalisation is to replace the system level train risks with the root causal failures using the trace and rationalisation process described in Appendix J. Appendix E shows how the CAM-C has been used to create a system level FMEA. The occurrence level of the causal failures was adjusted to take account of the amplification effects using the process described in Appendix J. There were no resistive links in the CAM-C and therefore effects from causes fed straight through to system level failures unchecked. The amplification factors were fed through the system to the 'system level' and the occurrence rate adjusted by doubling it by the number of times indicated by the figure in the adjust at system level column using the process described in Appendix J.

Commentary

The simplification of the train considered the train subsystems as a single system by considering any row with an entry in the 200 series as a single row for the purposes of tracing. For example, entries in column 106 corresponding to the train subsystem were considered a single entry, using the highest level linkage as the overall factor; in this case, a 3. This strategy simplified the analysis and switched the focus to the infrastructure.

CAM-Stage 5

Key points summary

As shown in Appendix E, the system level FMEA was converted to a cause-consequence table to provide the summary of risk with 8 individual hazards and 14 causes. It indicates that all the risks were intolerable, driven by the lack of effective controls. This is to be expected in an uncontrolled critical system.

Judgement of the Author was used to deal with hazards 401 and those in the 500 range. They have been judged as having a critical consequence overall because they will be applied throughout the organisation. It is likely that the effects of shortcomings in these areas will credibly be felt in less serious incidents. Those processes concerned with the implementation (400 series) have been, with the exception of 401, been judged to have a catastrophic consequence because they are specifically concerned with the set of points in the incident.

The Management summary risk matrix, Table 59 shows that all the risks are intolerable hazards. This result aligns well with the RAIB investigation and the assumptions about reliance of railway switches on maintenance. The switch risks are only tolerable if the controls are applied which according to the RAIB report they were not.

Typically, when examining a system, a distribution of risks would be expected to some extent across the likelihood/ consequence spectrum. However, in this case, that characteristic is absent. Instead, the absence is likely to be a characteristic of the RAIB source data being 'cleansed' of those factors that are not at high risk to convey a focused message about the incident

Table 59 Grayrigg risk matrix reproduced from Appendix E

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent				401, 504, 505	102, 103, 106, 402, 403, 404
Probable				501, 502, 503	101, 105,
Occasional					
Rare					
Improbable					
Highly Improbable					

Commentary

The collection of failures and of the addition of an extra column indicating the number of category increases in the overall FMEA simplified the conversion task of the table into hazards. In addition, the conversion to a cause-consequence table and adjustment to show the system-level effect of the integrated parts could have been undertaken in one step. However, in the Author’s opinion, the single-step approach could have led to increased errors due to the increased complexity. Therefore, the two-step approach appears superior.

8.2.4 Findings from study and lessons learned

Table 60 Comparison of findings

RAIB finding summary			New CAM method	
Ref	Primary causal factor	Secondary causal factor	Findings	Commentary
1	Points 2B were in an unsafe state		The new method identifies that the points could be in an	The amplification of the switch part risks through the CAM-C

RAIB finding summary			New CAM method	
Ref	Primary causal factor	Secondary causal factor	Findings	Commentary
			unsafe state and assigns an intolerable risk to each, for example 105. This represents that if the rails move due to defective point parts the train is likely to climb the rails and derail.	serve to highlight the criticality of these risks
2	Restraint of the left-hand switch rail had been lost	Stretcher bar assemblies had failed	The new method identified the key role of the stretcher bar 101, 102	The amplification of the CAM-C stages serves to show that the stretcher bars were a key risk.
3	Degradation of the third stretcher bar was undetected		The new method identified the risk of missing tasks and inspections 501-505	CAM shows the criticality of the inspections to the integrity of the points and in particular the stretcher bars. This is evident from the CAM-C that clearly shows that risk 102 is critically dependent on the inspections
4	Excessive switch opening 10mm through incorrect gap		This risk is identified in 106	
5	Missed visual inspection on 28 February 2007 removed opportunity to spot degradation		This is identified in 404 and 505 where the risk of too much work for the hours and resources were identified	CAM goes further than the finding by also identifying the volume of work as a vital parameter.
6	Constraints from access problems and combined inspection on 18 February contributed		The new method identifies that the process constraints are a risk both to normal work 501 and critical tasks 505	

RAIB finding summary			New CAM method	
Ref	Primary causal factor	Secondary causal factor	Findings	Commentary
7	Omitted inspection not identified	Records incorrectly updated	The new method correctly identifies that detection of omission is low	

Overall, there is a good match by using the new method. In addition, the method has identified that the new measurement train data could be a strong control, as long as users are not overloaded with data. This would provide another source for indications. If the data were used the effect of the track patrols would be reduced and the undetected deterioration effects of missed maintenance would be similarly reduced. This was not highlighted by the accident report. This has been a time limited analysis and more could be learned about the accident if a more in-depth study were carried out. However, the results demonstrate the value of CAM and the capability to identify key aspects of accidents.

Given that the method successfully identified the main findings in the official report, it is concluded that the method is at least on a par with those used in producing the report.

Furthermore, the method was straight forward to use and appears to address the criticism levelled by Underwood and Waterson (2013b) that the modern methods they tested were difficult to apply.

8.2.5 Research success criteria satisfaction

This section reports the Grayrigg test case satisfaction of the specific success criteria set in Table 57 of Section 8.2.1. Three criteria were set to gauge the success of CAM, Table 61 below summaries how these were fulfilled in this application and the extent to which the criteria were achieved.

Table 61 CAM application success measure

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
Safety	<ul style="list-style-type: none"> As a minimum the same hazards and or causes are identified in the official report 	<ul style="list-style-type: none"> The application analysis has identified the findings in the official report and additional hazards as described in Table 60. CAM identified at least one risk for each finding in the RAIB report. CAM identified the New Measurement Train data as a critical causal risk. This risk was not highlighted in the RAIB report 	Number risks identified	Yes		14	Surpassed expectations
			Number of official finding risks missed	Yes		0	
			Number of additional hazards identified	Yes		1	
Economic	<ul style="list-style-type: none"> An efficient method of performing the analysis. No high-powered computers or 	<ul style="list-style-type: none"> The test case has demonstrated an analysis without specialised computing support. 	Estimated analysis time		Yes	2 days	Successful
			Approximate number of	Yes		21	

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
	<p>software packages required.</p> <ul style="list-style-type: none"> • Time to complete is less than 5 days. • Analysis pages to be less than 50. 	<ul style="list-style-type: none"> • It has shown that the salient subsystems and their relationships were identified. • The flexibility of the CAM model allowed the train to be treated as a single entity with multiple inputs without deflecting attention from the infrastructure. • The analysis quickly focused on the critical relationships. • No complicated maths was required. • The duration of the analysis was within the time limit. 	analysis pages				
Applicability	<ul style="list-style-type: none"> • Applicable to railway engineering safety risk assessment problems with 	<ul style="list-style-type: none"> • The successful identification of the risks with the Grayrigg test case has demonstrated that CAM can be 					Successful

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
	single and multiple systems.	<p>used with multiple separate systems that include physical features and people as evidenced by the CAM-ERD.</p> <ul style="list-style-type: none"> This test case has shown that primarily process based incidents can successfully be analysed with CAM 					

8.3 CAM benchmark using the Grayrigg results

Underwood and Waterson (2013b) created a benchmark to determine whether various risk analysis techniques incorporated 'systems thinking' into accident analysis. This section carries out that same process on CAM with a view to extrapolating the statement to system risk analysis in general. Three objectives were set for their study:

1. To analyse the accident.
2. Compare the method's performance against a framework.
3. To 'reflect on the similarities and differences' between the methods.

Item 1 is satisfied by Section 8.2 and Section 7.3 of Chapter 7. Item 3 has been largely satisfied through the comparative case study undertaken in Chapter 7. This section will explore item 2.

Underwood and Waterson (2013b) describe two major axes for their framework, systems thinking and usage characteristics. The paper goes on to describe the attributes associated with each, and where appropriate the properties of the attribute. The paper provides a descriptive assessment of each for the studied methods. These measurement attributes are applied by the Author to CAM in this section.

Systems thinking

This measurement axis is concerned with features of the method and how they align to the systems philosophy.

Table 62 CAM systems thinking assessment adapted from (Underwood and Waterson, 2013b)

Attribute	Short description	CAM assessment	Justification for assessment
System structure	<ol style="list-style-type: none"> 1. The definition of a boundary 2. The hierarchy level (subsystems) 3. The system goals and objectives 	<ul style="list-style-type: none"> • The boundary of the system is defined in CAM-ERD. The subsystems and interrelationships are also depicted in the CAM-ERD. The nature of the risk relationships is shown in the CAM-C by indicating how subsystems are linked together and the type of link. • The analysis can be tailored to be centred on the system goals and the risks associated with those goals. 	<p>The purpose of CAM-ERD is defined in Chapter 6 and is stage 1 of the CAM process, an example is shown in Figure 36. This is a form of an entity relationship diagram that deals with subsystems and links between them. Also, CAM-ERD defines a boundary for the system in the diagram.</p> <p>CAM-ERD has a particular symbol for a point of harm to focus the analysis, which is regarded as the goal for the risk analysis. Furthermore, CAM-ERD is not restricted to physical entities and can also represent concepts and functional goals. CAM-C is a combinator and by its nature will define a link between two entities. The scaling of CAM-C is defined in Chapter 6. It defines the nature of the relationship.</p>

Attribute	Short description	CAM assessment	Justification for assessment
System component relationships	<ol style="list-style-type: none"> 1. Emergent behaviour from interactions 2. Holistic view of system 	<ul style="list-style-type: none"> • CAM incorporates iterative loops in the analysis. Also, CAM has a stage for subsystem analysis followed by the CAM-C combinator and then a system level analysis, which will enable emergent behaviour to be analysed • CAM-C describes the whole system in terms of risk relationships 	<p>Chapter 6 defines CAM as consisting of an iterative process which consideration of changing/emergent behaviour which is described in Section 6.3.4.5. Moreover, the process specifically has a system level stage.</p> <p>The CAM iterative process requires that the risk analysis process is reviewed and adjusted by rerunning stages 1-4.</p>
System behaviour	<ol style="list-style-type: none"> 1. Environmental conditions accounted for 2. Transformation of inputs to outputs to achieve system goals 	<ul style="list-style-type: none"> • CAM-ERD enables the incorporation of environmental factors to be included in the analysis by simply creating a virtual subsystem for the environment • CAM-C is a vehicle that enables risks to be transformed from inputs to output level risks. 	<p>Chapter 6 includes an example in Section 6.4 which includes environmental factors. The case study in Chapter 7 demonstrates the transformed risks from a low-level input system to the effect on the high-level system. CAM-C was used to map the transformation relationships through the process defined in Chapter 6 for stage 3.</p>

Usage characteristics

This measurement axis is concerned with the requirements placed on the user and the utility of the output.

Table 63 CAM usage characteristics assessment adapted from (Underwood and Waterson, 2013b)

Attribute	Short description	CAM assessment	Justification for assessment
Data requirements	<ol style="list-style-type: none"> 1. Types of information required 2. Information required for an analysis 3. How data is processed 	<ul style="list-style-type: none"> • CAM requires information on the system composition. Also, CAM requires risk information for each of the subsystems (or subcomponents). • A reduction in the information available will reduce the depth and possibly quality of analysis, but it does not prohibit an analysis. • The choice of subsystem analysis tool will determine the exact nature of the data required. • The data is processed initially in parts and then brought together using the CAM-C to form a holistic picture. 	<p>CAM-ERD is used to define the system to be analysed. Once defined this is used to decompose the system into analysable subsystem parts. A lack of detail will limit this step and will reduce the depth of the following analysis.</p> <p>As described in Chapter 6 CAM can use a number of established techniques for stage 2 of the analysis. The choice by the analyst will determine the data requirements. Furthermore, CAM is designed to allow qualitative or quantitative analysis.</p> <p>Chapter 6 defines a process that initially decomposes the system into understandable subsystems and then uses the CAM-C to bring the results together before further analysis at the system level. Chapter 6 provides for data transformation in the scheme.</p>
Validity and reliability	<ol style="list-style-type: none"> 1. Is the method valid and reliable 	<ul style="list-style-type: none"> • The original paper states that providing internal validity is not possible. However, in the case of CAM external validity for 	<p>The test cases contained in chapters 6, 7, 8 and 9 show that CAM produces justifiable output. However, this does not absolutely prove it will work in every case</p>

Attribute	Short description	CAM assessment	Justification for assessment
		<p>the Baildon and Grayrigg test cases is established through comparison with the RAIB findings.</p> <ul style="list-style-type: none"> Likewise, CAM has not failed to produce output aligned to the RAIB output and is considered reliable 	<p>due to the limitations of the assurance strategy adopted.</p>
Usability	<ol style="list-style-type: none"> Is it easy to understand and apply? Is guidance and training available 	<ul style="list-style-type: none"> CAM appears to be understandable and breaks the analysis down into manageable parts Since CAM uses established techniques for the subsystem level analysis there are training courses and guidance for these elements. However, there is currently no training available for CAM as a whole. 	<p>CAM has taken the approach of breaking the problem into parts and encapsulating the analysis of each part. This is described in Chapter 6 for stage 2 of the process. According to (Manson, 2001) reductions of complexity will increase understanding.</p> <p>CAM is a new process and it is justifiable that training is yet to be established.</p>
Graphical representation of the accident	<ol style="list-style-type: none"> Is the accident/incident graphically represented Is the output charted or represented in a communicable way 	<ul style="list-style-type: none"> The CAM-ERD provides a diagrammatic view of the system and the points of harm. CAM-C is a semi-graphical method of 	<p>As described in Chapter 6 CAM has been designed to use diagrams and matrices that pictorially show relationships. In addition, CAM-C when rationalised is colour coded to indicate the significance of the link. Moreover, a colour coded risk matrix has been included as a</p>

Attribute	Short description	CAM assessment	Justification for assessment
		<p>demonstrating influence in the system</p> <ul style="list-style-type: none"> <li data-bbox="943 347 1335 493">• The risk matrices are a pictorial method of describing risk in the system 	<p>communication tool to relate the risk to the level of acceptability.</p>

8.3.1 Summary

From Table 62 it appears that CAM meets the systems thinking concepts as set out in the table. It is able to express the system as a whole and as its component parts. The analysis takes a holistic view of the system under analysis. Table 63 indicates that CAM has positive usability characteristics, although the training element is currently not available. A strength appears to be the use of diagrams and matrices to simplify the presentation of risk propagation through the system.

Section 8.2.4 indicates that CAM has identified similar findings to those of the official RAIB report. It appears that CAM has been more effective in some areas by identifying additional risks, for example as noted in the findings of Chapter 7.

Chapter 7 has shown that CAM performs well when compared with other techniques such as STPA and YB. The current techniques, for example FMEA, incorporated into CAM have combined to produce a rich risk data set which is filtered to show the salient risks.

Overall CAM meets the requirements for 'systems-thinking' and usability.

Furthermore, CAM appears to perform favourably, when compared with the analysis techniques of STAMP, SCM, and Accimap used in the study by Underwood and Waterson (2013b).

8.4 Hong Kong metro incident CAM application test case

The Author has applied CAM to a test case on a mass transit metro railway system using CAM in the reverse direction, the CAM-RA variant; this analysis works back from an accident towards the root causes. The test case accident occurred during system testing and resulted in a train collision. The focus of the

analysis concerns a modified software train control system which is more dependent on processes than the physical systems of the previous applications. Accordingly, it provides an application example of a process driven system.

An objective of this application is to identify the conditions to permit an acceptably safe resumption of testing and summarise the critical risk causes. At the time of the analysis members of the university needed to know what to suggest for the control system testing to safely commence and it was thought CAM could provide an answer.

The full analysis is contained in Appendix F, a summary of the key points from the CAM application is explained in this chapter subsection.

8.4.1 Test case success criteria

The measures of success for a case study were defined in Chapter 1 Section 1.9 as Safety, Economic and Applicability, which for this case are interpreted as shown in Table 64.

Table 64 Success measure interpretation

Measure	Interpretation
Safety	The CAM analysis should indicate the where the mitigations need to be applied for safe testing to recommence.
Economic	The process should be understandable and relatively effortless to implement without resort to specialist tools, such as specialist software packages or high-powered computers. Also, it should be possible to complete the analysis with a reasonable timeframe; within 3 days. Moreover, the analysis should be less than 50 pages.
Applicability	The process should be directly applicable to the railway environment without additional adaption.

For this analysis most the measures are subjective because there is no reference comparator for the output, consequently measures are demonstrated through illustration and success is judged subjectively by the Author.

8.4.2 Method used

The analysis method used is as explained in Chapter 6, Section 6.4.2 and labelled as CAM-RA (Post accident reverse analysis). The process is reproduced in Figure 37 for convenience and the user instructions can be found in Appendix J. The Author has decided for the purposes of this test case that the CAM-RA variant appropriate because a report of the facts of an accident have been provided and the objective is to decide about the risk posed going forward.

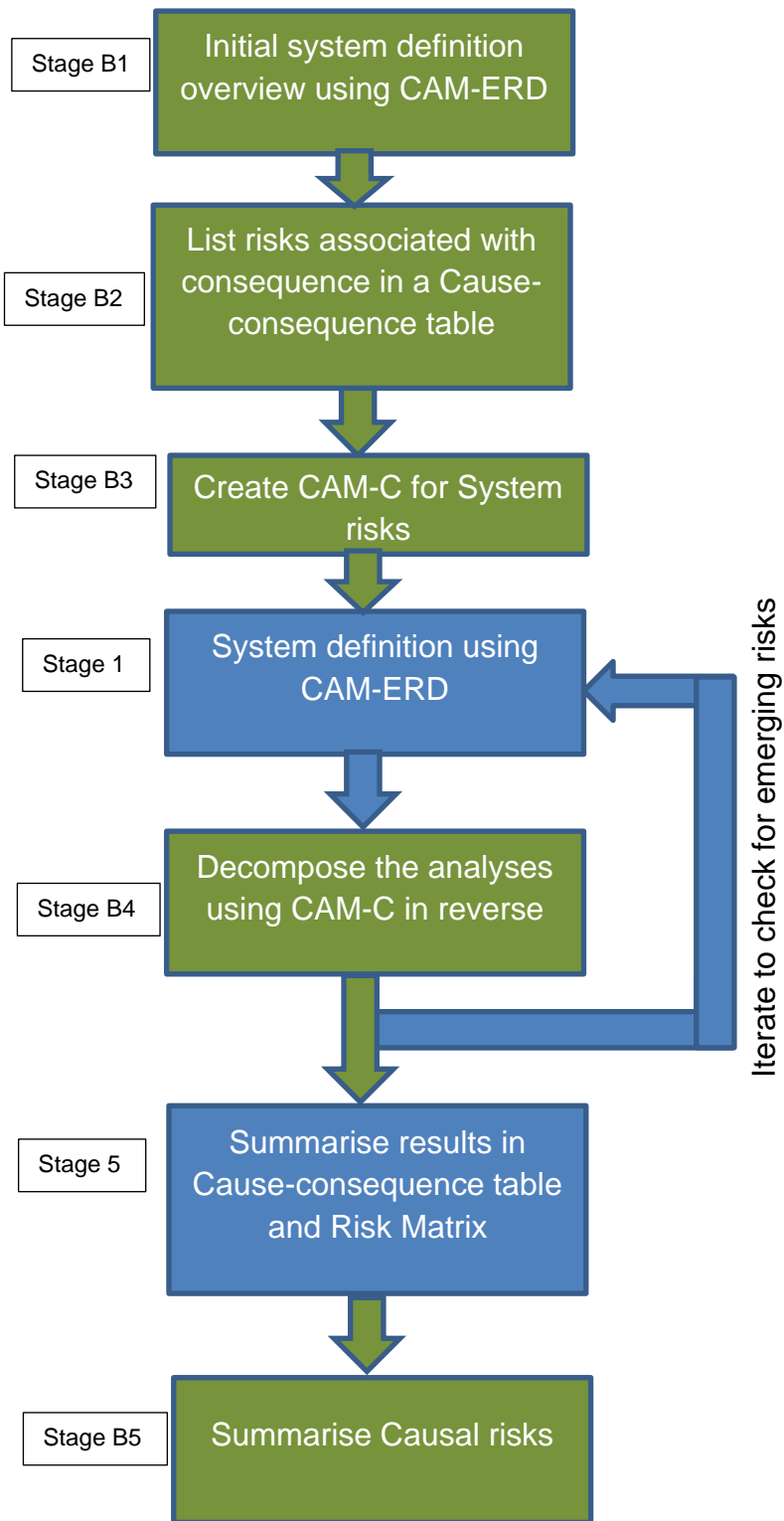


Figure 37 CAM_RA process reproduced from Chapter 6

The steps to carry out each of the stages listed in Figure 37 are described in Appendix J.

8.4.3 Brief accident summary

A full accident description is contained in Appendix F.

The incident took place during testing of a new signalling system on the MTR Tsuen Wan Line in Hong Kong. The system is an automatic metro CBTC system which has been designed for high efficiency. Extra features were contracted to provide resilience when a failure occurred and avoid down time, effectively, masking failures from the public. This resulted in a novel design using three zone controllers instead of the usual two. Two trains collided on a cross-over, because the zone controller did not register that the crossover was already occupied before routing a second train onto the cross-over. The accident happened during the testing of the novel third zone controller.

8.4.4 Source of information

A report has been produced by the Hong Kong authorities (Electrical and Mechanical Services Department, 2019); currently this is the only source of information apart from news reports which appear to be drawn from the same source. Some general information is available on the contractor's Thales zone controller system from a presentation given to the Institution of Signalling Engineers (Thales Group, 2015). Therefore, the information is limited which has constrained the analysis.

The accident report referenced the signalling standard EN50129 (CENELEC, 2003) and a metro standard IEEE1474.4 (IEEE, 2011), which specifically deals

with testing of CBTC systems. EN50129 is used to point out that a safety case is required, while IEEE1474.4 is used to highlight the need for operational testing.

8.4.5 Analysis

The analysis is fully described in Appendix F, this section contains summarised key points and commentary to illustrate the application of CAM and its features. A heading in bold and underlined is provided for each process stage as an aide to follow the process laid out in Section 8.4.2.

Stage B1

Key points summary

The overall system comprises a number of subsystems as shown in the CAM-ERD, which has been created by using the accident information provided and decomposing the railway into salient subsystems. In a CAM-ERD subsystems are represented by circles and parts by rectangles, the point of harm is identified by a red triangle. Relationships are represented by arrows and normally labelled with risks, although other labels can be used to help the understanding. The CAM-ERD is fully explained in Appendix J.

In a departure from the instructions in Appendix J the subsystems are not identified by circles because the information did not lend itself to that layout and the relationships are predominantly functional. The parts identified by colour coding the 'level' of the subsystem. Yellow denotes the system level components (possibly major subsystems), brown are key parts that are linked to the system level components. The beige colour are lower level parts.

It is relatively easy to redraw the CAM-ERD with the subsystems shown as circles, but the Author judged that there was no further value obtained from this additional step. The resulting CAM-ERD is shown in Figure 38, where the interrelationships between the various infrastructure systems and parts are clearly identified.

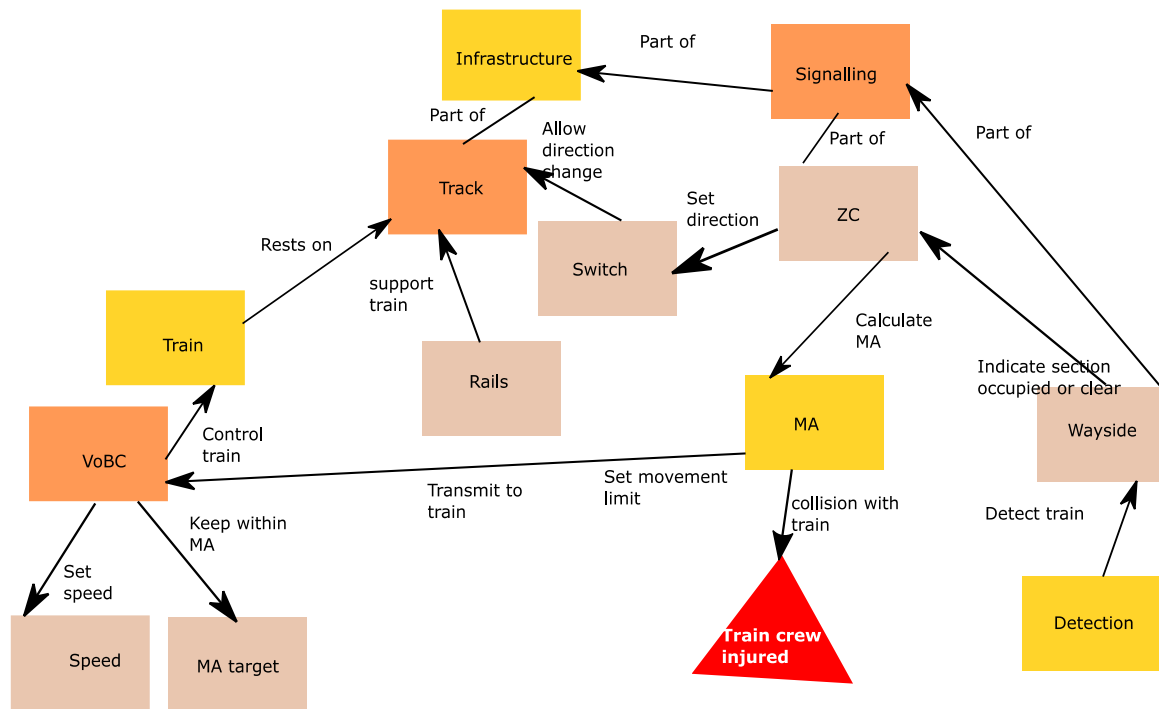


Figure 38 CAM-ERD overview relationship diagram from Appendix F

As can be seen from Figure 38, the zone controller (ZC) is essentially at the heart of the system, receiving information about track occupancy, setting routes through the switch control and issuing movement authorities (MA) to trains. It also indicates that the MA if incorrect can cause a collision.

Commentary

The available documentation does not lend itself to dividing into a tidy subsystem-based drawing. However, by colour coding the parts, it was possible to group them into train-based, infrastructure-based and signalling-based clusters. These translated to infrastructure, train, MA, and detection subsystems. The Author

considered that the resulting diagram was good enough to convey the necessary relationships required from a CAM-ERD for the next stage.

8.4.5.1 Process approach

Using CAM in reverse mode, CAM_RA, the analysis works back through the system in an iterative manner, passing through a number of cycles, where the focus of each cycle is guided by the previous one.

Stage B2

Key points summary

A simple cause effect table is constructed as a first stage in the analysis from the CAM-ERD, shown in Figure 38. An extract from Appendix F is shown in Table 65. Normally, these tables are supported by thorough analysis documentation and the tables include mitigations, and barriers which are omitted from all bar the final stage. The notes in this table were used to indicate whether there was evidence from the accident report (Electrical and Mechanical Services Department, 2019) to support the hazard.

Table 65 Extract of system level cause-consequence table

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
101	Trains off track	Track fails	The track formation fails and train leaves track and continues on ballast	Train collision	<ul style="list-style-type: none"> Track design Train speed Inspection 	Highly Improbable	Major	Tolerable	<ul style="list-style-type: none"> It is clear that this did not happen as the track was intact
106	Faulty MA issued	Zone controller malfunction	The zone controller issues an MA which is not valid and is in conflict with another train	Train collision	<ul style="list-style-type: none"> Zone controller is a high integrity unit and is a 2oo2 	Improbable Probable	Catastrophic	Tolerable Intolerable	<ul style="list-style-type: none"> The MA should not have been issue to train when crossover occupied

Commentary

The production of the cause consequence table involved considering each major subsystem in turn. First, possible causes were generated from the accident report using railway knowledge and themes. Next, the likely risk was estimated using railway experience. This task would be difficult without railway knowledge, even with the aid of the CAM-ERD, because of the requirement to estimate risk and cause.

The resulting table creates a starting point for the following tracing process.

Stage B3

Key points summary

This stage of the process is explained in Appendix J. The analysis contained in Appendix F has shown that a useful modification is to append an evidence indicator to the CAM-C combinator to reduce effort spent on unsupported investigation. A CAM-C, as set out in Table 66, is used to focus the investigation on the key items from the overall systems analysis. This CAM-C combinator is slightly different to the others because the columns are populated with consequences. It creates the mapping back to the system level hazards to initiate the iterative CAM process; in effect it primes the CAM-C matrix.

Table 66 Reproduced CAM-C system level hazards – consequences

			Consequence property			
			Evidence	train out of control	MA incorrect	lineside error
Hazards	101	Trains off track	No			Yes
	102	Switch setting wrong	No			Yes
	103	Train speeding	No	Yes		
	104	Train speeding leaves track	No	Yes		
	105	Train outside MA	No	Yes		
	106	Faulty MA issued	Yes		Yes	
	107	Zone controller faulty start up	Yes		Yes	
	108	No train detected	No			Yes

The evidence column of Table 66 is populated with a ‘Yes’ when there is a statement in the accident report that gives an indication that the hazard was realised. As can be seen there are only two system level hazards (106, 107) that are relevant to the current investigation (supported by evidence and connected with an incorrect MA). It indicates that the subsystem of interest is the zone controller.

Commentary

The creation of the CAM-C at this stage was a matter of extracting the relevant rows from the cause-consequence table. The more difficult task was to identify the significant risks. The introduction of an evidence column simplified the task because it was easy to see which hazards were supported by evidence.

Subsequently, the accident report was reviewed to establish if the hazard was identified either explicitly or implicitly.

Stage 1

Key points summary

The Author generated a reformulated CAM-ERD in Appendix F, which is reproduced in Figure 39, and used it to develop the next level of the analysis with the focus set to the zone controller because Stage B3 indicated this was a critical part.

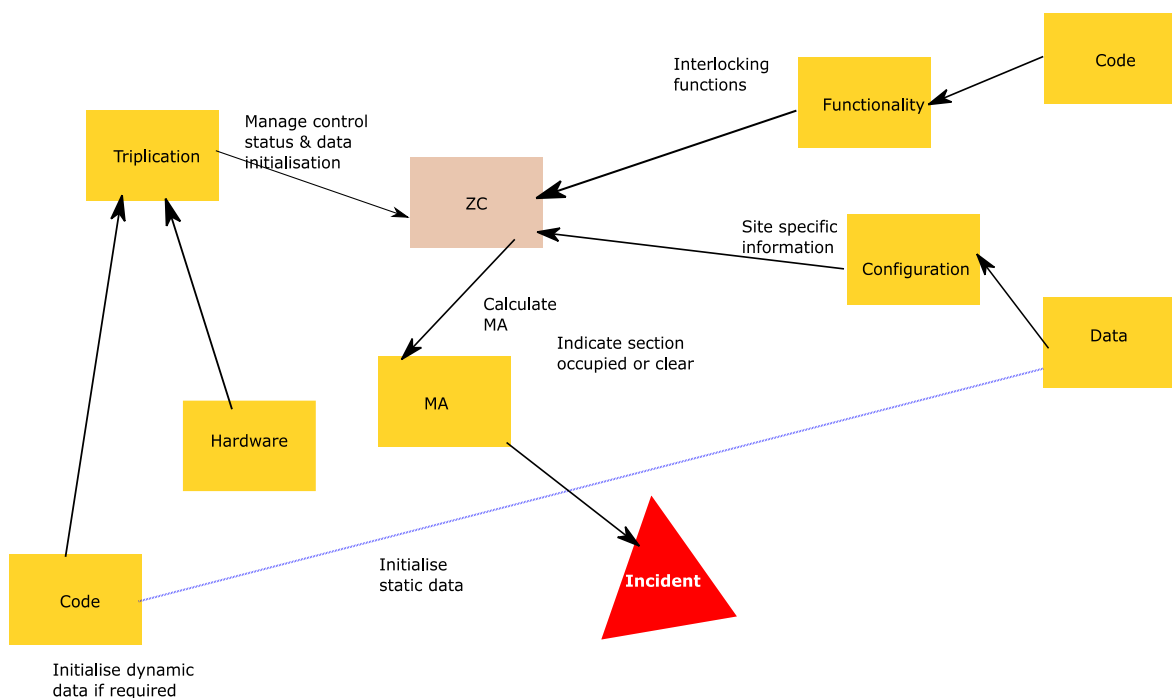


Figure 39 Developed CAM-ERD focused on the controller

As can be seen from Figure 39, the details of the controller are developed to a lower level. It is clear that software and data play a critical role in the system.

Commentary

The revised CAM-ERD was formed by taking the subsystems identified in the previous stage and extracting additional information from the documentation about

the control system. Consequently, it established the inter-relationships between the lower-level subsystems.

The resulting diagram appears to provide the necessary information for the following process stage.

Stage B4

Key points summary

The CAM-ERD, Figure 39, was used to amend and develop the cause-consequence table. An extract from Appendix F final cause-consequence table is shown Table 67. The table shows the altered likelihood (in red) at the system level due to the effect of amplification through the system and consequently the resulting risk. It is of particular note that for some of the hazards the likelihood increased by several orders, which had a major impact on the overall understanding of risk.

Table 67 Extract from Appendix F Reformed cause-consequence table indicating the effect of amplification

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
201	Controllers differ	The software has latent errors	The software managing the status of each controller has errors which causes the 'view of the railway to differ'	When the controllers swap master function there is a difference causing an unsafe state	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 IEEE1474 	Improbable Probable	Catastrophic	Tolerable Intolerable	<ul style="list-style-type: none"> This is in effect what happened as stated in the evidence. Therefore, the controls are not effective or were not implemented properly.
202	New software unproven	The software has latent errors	The software is changed and novel functionality is introduced	The software malfunctions causing an unsafe state	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 IEEE1474 	Occasional Frequent	Catastrophic	Intolerable	<ul style="list-style-type: none"> This is what happened as stated in the evidence. Therefore, the controls are not effective or were not implemented properly.

The final CAM-C extracted from Appendix F is shown in Table 68 which was developed with the adjusted cause-consequence table, (extract shown in Table 67). This demonstrates the iterative nature of the analysis. Further iterations could have been undertaken if additional evidence was made available. The analysis is terminated at this level and a mitigation table is populated to indicate the steps necessary to reduce the risk to acceptable levels. Carrying the analysis further would have resulted in unsupported speculation by the Author.

Table 68 CAM-C for Zone controller - system level hazards

			System level hazards								
			Evidence	Trains off track	Switch setting wrong	Train speeding	Train speeding leaves track	Train outside MA	Faulty MA issued	Zone controller faulty start up	No train detected
				101	102	103	104	105	106	107	108
Controller Hazards	201	Controllers differ	Yes						3	3	
	202	New software unproven	Yes						2	3	
	203	Varying critical new functionality	Yes							3	
	204	System untestable	No						3	3	
	205	Live system has unproven data	No						2		
	206	System does not meet integrity level	Yes						3	3	

Key	
3	- Amplifier
2	- Carrier
1	- Resistor
-10	- Terminator

Table 68 shows that the issuing of an MA and the faulty start up were critical failings in the subsystem that were responsible for the accident.

Commentary

The modified cause-consequence table was created by applying the CAM-C to the initial values. The CAM-C, in this case, was created by assessing the linkages between the parts using the documentation, implicit railway domain knowledge and logical deduction.

The resulting table appears to focus on the zone controller and establishes the parameters for the next iteration.

Stage 5 and B5

Key points summary

Appendix F contains the additional mitigations to reduce the likelihood of the key hazards and therefore reduce the risks to an acceptable level to meet the objective of identifying how to safely restart testing. These mitigations counter the system developer's non-compliance with the software assurance process that occurred. The mitigations are as follows.

Table 69 Mitigations identified in Appendix F

Hazard	Mitigation
107	<ul style="list-style-type: none">• Zone controller to be tested on a reference layout
201	<ul style="list-style-type: none">• Design to be amended for a consistent view• Logic and hardware to be used to determine status

Hazard	Mitigation
202	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout. • All code to be exercised at the modular level. • Critical code to be tested and documented at the system level • Code constructed with defensive programming techniques
203	<ul style="list-style-type: none"> • Architecture to be modified to produce a consistent set of functionalities. • Logic and hardware to be used to determine status
204	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout • Safety critical system complexity to be reduced as far as possible
205	<ul style="list-style-type: none"> • Pre-commissioning testing of data • Hand checking of data by competent persons • Data to be simplified to a minimum • Untestable data to be eliminated • Testing of operational scenarios • Comparison of data with the old system
206	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout. • All code to be exercised at the modular level. • System functionality to be kept to a minimum • Independent testing by an external body to take place

The pre- and post-mitigation risk mapping is reproduced from Appendix F in Table 70 and Table 71.

Table 70 Pre-mitigation risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					202, 204, 206
Probable					106, 107, 201
Occasional					
Remote					203, 205
Improbable					102, 103, 104, 105, 108
Highly Improbable			101		

Table 71 Post-mitigation risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent	Yellow	Red	Red	Red	Red
Probable	Yellow	Yellow	Red	Red	Red
Occasional	Yellow	Yellow	Yellow	Yellow	Red
Remote	Green	Green	Yellow	Yellow	203, 204
Improbable	Green	Green	Green	Yellow	102, 103, 104, 105, 106, 107, 108, 201, 202, 203, 205, 206
Highly Improbable	Green	Green	101	Yellow	Yellow

These matrices clearly show the grouping of the hazards identified and that the critical ones (in the range 200) concern the zone controller. Table 71 shows the mitigated risk profile and although the potential consequences of a risk materialising is catastrophic the risk is tolerable. The high consequence outcomes are to be expected for a mass transit safety critical system.

Commentary

The mitigations were identified by reviewing the applicable standards and adjusting the likelihood to consider the anticipated effect. This task was straightforward for this case because the computer-based control system requirements are tightly specified in standards. However, it may be more difficult for other types of systems.

The resulting diagram provides a pictorial illustration of the risks that point to the zone controller's failings.

8.4.6 Findings from application and lessons learned

The following was concluded from the CAM application undertaken in Appendix F:

Findings

- 1) CAM is capable of being applied to other railway types apart from the GB mainline.
- 2) It is possible to apply CAM in reverse mode, working back from an incident/accident.
- 3) Mitigations were identified using the analysis which indicates that they will reduce the risks to an acceptable level to recommence testing.

Lessons learned

- 1) The initial CAM-ERD (relationship diagram) is central to the subsequent study. It is worth taking some time to get this stage right. Initially, the CAM process did not contain this stage. The process has been amended to incorporate it by altering Chapter 6 and Appendix J.
- 2) The initial CAM-C is a little false, in the sense that it is not a system/subsystem or subsystem relationship. However, when driving the process in reverse from an incident there must be a translation stage to initiate all the other CAM-Cs used in later stages of the analysis. The difference has been incorporated into the process description and highlighted with an example in Appendix J.

- 3) When working in reverse mode it is more efficient to include the evidence as part of the initial CAM-C to focus the study, otherwise effort is potentially wasted following and eliminating false trails at a later stage in the analysis. The use of an 'evidence' flag has been incorporated into Chapter 6 and Appendix J user instructions.
- 4) Rationalisation does not need to be explicitly applied because it is an implicit part of the reverse process.

8.4.7 Research success criteria satisfaction

This section reports the on the satisfaction of the specific success criteria for this test case application of CAM set in Section 8.4.1. Table 72 below summarises how these three criteria were fulfilled and the extent to which the criteria were achieved.

Table 72 CAM application success measure

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
Safety	<ul style="list-style-type: none"> The analysis is to indicate where mitigations are need for safe testing to recommence. 	<ul style="list-style-type: none"> The application analysis has identified appropriate hazards as described in Section 8.4.6 Mitigations were identified using the information from CAM and it was shown that the modified risks were acceptable. 	Number risks identified	Yes		14	Successful
Economic	<ul style="list-style-type: none"> An efficient method of performing the analysis. No high-powered computers or software packages required. 	<ul style="list-style-type: none"> The test case has demonstrated an analysis without specialised computing support. It has shown that the salient subsystems and their relationships were identified. 	Estimated analysis time Approximate number of analysis pages	Yes	Yes	1 days 25	Successful

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
	<ul style="list-style-type: none"> Time to complete is less than 3 days. Analysis pages to be less than 50. 	<ul style="list-style-type: none"> The Author was able to reconstruct the relationships between the subsystems using the reverse CAM method. The analysis quickly focused on the critical relationships. No complicated maths was required. The duration of the analysis was within the time limit. 					
Applicability	<ul style="list-style-type: none"> Applicable to railway engineering safety risk assessment problems with single and multiple systems. Ideally, to also be applicable in other fields 	<ul style="list-style-type: none"> This application has demonstrated that it can be used with multiple separate systems. There has been a demonstration that the it is applicable to software processes and metro systems. This test case has further demonstrated that primarily process 					Successful

Category	Criteria	Measure					Satisfaction Level
		Observations	Numerical measures	Objective	Subjective	Value	
		based incidents can successfully be analysed with CAM					

8.5 Summary and conclusions

The CAM test cases analysed in this chapter have demonstrated that CAM can be applied reliably to different scenarios. One of the illustrative applications has served to demonstrate that CAM can be applied to metro as well as GB mainline cases. In each case all the satisfaction criteria were satisfied. This success provides evidence that CAM is a method that incorporates generic principles and could be widely applied. In each case annotations were provided to indicate that a predetermined process was being followed. Furthermore, the benchmark analysis undertaken in Section 8.3 provides additional evidence that CAM meets the criteria for a 'systems thinking' method of analysis. This analysis appears to place CAM at least on a par with the modern techniques such as FRAM.

The applications have shown that two different variants of CAM have been successfully applied. It is clear from the results that the CAM reverse mode is efficient in tracing back from an accident and identifying root causes, using only 25 pages to achieve the task.

There have been learning points from the case study which are described in Section 8.2.4 and Section 8.4.6 as:

- a) In the reverse mode (CAM_RA) the initial CAM-ERD is central to the subsequent study;
- b) In the reverse mode (CAM_RA) the initial CAM-C must use the consequences to link to system level hazards to prime the subsequent development of the CAM-C;

- c) Efficiency in the reverse mode (CAM_RA) is improved by including a flag to denote that hazards are supported by evidence.

These have been incorporated into the method by altering Chapter 6 and Appendix J. Consequently, the method is now more robust.

The test cases have increased confidence that CAM is applicable to different scenarios and thereby increased the external validity of CAM.

9 Conclusions and further work

This chapter lays out the conclusions of the thesis as a series of parts:

- An overall high-level conclusive statement;
- A review of the essential points supporting the high-level statement;
- A justification of the satisfaction of subsidiary questions;
- Weaknesses and shortcomings;
- Further work;
- Final conclusions.

Together, they form a considered conclusion to the research undertaken, linking together the core output and conclusions from previous chapters to form a rational, logical culmination of the thesis.

9.1 High-level conclusive statement

In summary, this thesis has described research to investigate the question laid out in Chapter 1:

Can an understandable new method be developed to analyse and provide an overall risk estimation of system safety risk for railway systems comprised of one or more parts/subsystems that practitioners could use in the field?

Two subsidiary questions support the principal question:

1. How should safety hazards be combined in a safety analysis (i.e., where there is an interaction between the parts) to provide a credible overall risk picture without the requirement for expert knowledge?

2. Can a new method be created to identify safety hazards that other methods detect understandably?

Section 9.3 describes how these questions have been answered.

An explicit assessment of the need for a new safety risk assessment method was undertaken in Chapter 6 Section 6.1, using information from previous chapters. It concluded that the current methods leave a gap in safety analysis, and a new process is justified.

A proposed new method, CAM, allows existing methods and techniques to be used in parts of the analysis and has added several novel elements to the analysis process:

- CAM-C is a combinator adapted and customised from systems engineering DMMs/MDM into a safety analysis context. It acts as the 'flexible glue' between the various parts of a total system or process. Furthermore, it provides a codified process for combining subsystem analyses into a whole, which reduces process errors.
- CAM-ERD is a customised entity-relationship diagram similar to diagrams produced by Rasmussen (1997). These are adapted to show the point of harm, the information and physical linkages within an overall system.
- Rationalisation heuristics have been constructed to reduce the volume of data and focus the safety analysis on critical items. This feature assists in keeping the analysis process understandable for complex systems.

Confidence in CAM has been gained through several studies and a comparison with other contemporary methods to demonstrate that the method is useful, understandable, and provides acceptable results.

This thesis has satisfied the research questions in full, as described in Section 9.3; furthermore, as illustrated in Section 9.6, CAM represents a potential significant and useful advance on current risk analysis methods.

9.2 Review of the essential points and findings

Findings from the literature review indicate that the sociotechnical techniques emphasise the management and organisational risk. It has been shown that these are of less value in the railway environment because of the heavy regulation.

(Chapter 2 principal point i).

Although arguments can be made for other risk acceptance criteria, it was found in Chapter 2 that SFAIRP is a fundamental legal requirement that all valid risk assessments must meet. Furthermore, an explicit risk assessment approach avoids the risks of 'mispliance' of standards which supports the fundamental requirement for the continued use of these explicit risk assessment methods.

(Chapter 2 principal points ii, iii). CAM meets the requirements the legal requirements for a risk assessment technique.

Similarly, the arguments over probability and likelihood were found in Chapter 2 to be irrelevant. Processes like HazOp effectively pollute the purely mathematical approach. It was established that individuals express a belief about risk, and it is this strength of belief that is a critical input to a risk assessment, it is the relative scales that matter rather than absolutes. Consequently, analysis methods should be flexible.

In Chapter 5, it was discovered that a high percentage of GB rail incidents involved multi systems. A majority involved human errors, but even where safety systems were in place, a significant percentage involved component failures. (*Chapter 5, principal points i, ii, iii*). The findings indicate an industry where risks pervade all areas, and therefore providing a technique that only deals with a particular type of risk or single system is flawed.

Assessment of the various risk methods in Chapter 4 found that current methods emphasise various types of risk, for example, STAMP's managerial/organisational emphasis, and that a new method should allow the use of many different types as possible. Furthermore, it was discovered that most traditional techniques did not take a systems approach to analysis. (*Chapter 4 principal points vi, vii*). Therefore, these techniques are unsuitable for application in interconnected systems and system of systems applications without modification. CAM provides for multiple techniques in the subsystems analysis stage increasing the potential flexibility of the method.

Literature review findings show the criticisms of the traditional risk methods for sequencing are not well-founded. (*Chapter 2 principal point v*). The survey results in Chapter 4 have indicated that these traditional methods are the most popular and best understood by practitioners. The 'modern' techniques such as FRAM and STAMP are simply not popular. Furthermore, although parts of CSM are used for evaluation, they are not well understood. (*Chapter 4 principal points iii, v*). CAM has taken account of these findings by incorporating features that overcome these weaknesses.

Complexity has been established, in Chapter 2, to be a barrier to human understanding and risk assessment quality. It has been found that complexity in risk analysis can be controlled by undertaking subsystem analysis where the mechanisms are not as complicated. (*Chapter 2 principal points vii, viii*). This subsystem analysis feature has been incorporated in CAM and has been found in the test case of Chapter 7 to be valid. Furthermore, in Chapters 7 to 8, the CAM-ERD pictorial subsystem view of the system helped understanding.

Evidence has been presented in Chapter 2 to show that it is necessary to undertake a risk assessment at both the subsystem and system level to capture all the potential risks. (*Chapter 2 principal point vii*). In particular, it has been shown from the literature that complex systems have emergent behaviours that are not visible at the subsystem level. Chapter 7 findings have illustrated that a better result is obtained from CAM, which incorporates a system and system-level approach compared to other methods. Moreover, it has been found from Chapters 7 and 8 that CAM-C allows for whole-system analysis.

Three CAM variants were developed for efficiency reasons. These accommodate accident investigation scenarios, although all variants use common parts of CAM. Test cases in Chapters 7 and 8 have found that CAM produces good results in traditional rail risk applications, metro settings. These test cases have demonstrated that the CAM variants produce credible results.

The case study has found that CAM is more efficient and produces a better result than both the purely traditional approach, YB, and applying a STAMP variant.

The benchmarking findings in Chapter 8 provide additional assurance that CAM is a process-based technique and aligned with 'systems thinking'. It appears to compare well with the techniques examined in Underwood and Waterson (2013b).

CAM has been developed to recognise and incorporate the essential points drawn out earlier:

- allows the use of established methods and techniques;
- provides a method of combining subsystem analysis to facilitate a whole system analysis;
- encapsulates an emphasis on technical safety analysis while including human and organisation aspects;
- makes the problem understandable;
- simple to apply and efficient.

CAM is first developed in concept and then improved with feedback from the case studies in Chapters 7 to 8 into a refined process at the end of Chapter 6. The final version of CAM contains three paths that take account of new/updated developments and accident investigation scenarios. Therefore, the method is generally applicable to both predictive and deductive scenarios.

9.3 Satisfaction of research questions

This section describes the satisfaction of the main research question and the two subsidiary questions. Each answer draws on the evidence from the other thesis chapters.

Main question. Can an understandable new method be developed to analyse and provide an overall risk estimation of system safety risk for railway systems

comprised of one or more parts/subsystems that practitioners could use in the field?

Chapter 6 describes a new method, CAM, that shows the overall risk level, summarised in a risk matrix. CAM is a linear five-stage process with self-contained tasks and a feedback loop. The division helps the process to be more understandable. Furthermore, chapters 7 and 8 [Sections 7.3.5, 8.2.3 and 8.4.5] provide test case illustrations of the capability to analyse the overall risk. In each case, the analysed system contains several parts and subsystems.

Furthermore, the test cases were representative of actual accidents, as established in Chapter 5. Also, comparing the results of each CAM analysis of the GB mainline test cases with RAIB reports showed a good match. In some cases, CAM identified additional hazard causes. Consequently, there is a confidence that CAM does provide an estimation of the overall system safety risk.

Section 8.3 describes how CAM is potentially suitable for users in the field by satisfying Underwood and Waterson (2013b) systems and usability criteria. However, the development of training material remains an outstanding issue.

Subsidiary question 1. How should safety hazards be combined in a safety analysis (i.e., where there is an interaction between the parts) to provide a credible overall risk picture without the requirement for expert knowledge?

CAM incorporates CAM-C, described in Chapter 6 [Section 6.3.4.3], as the mechanism to combine the outputs from the various subsystems' safety analysis. It is based on a two-dimensional matrix, similar to a spreadsheet and is a development of the systems mechanism provided by Eppinger and Browning (2012). There is an interface between subsystems where a figure is in the corresponding intersecting cell. This feature graphically shows where the interfaces are, reducing the complexity of the analysis. The test cases in chapters 7 and 8 [Sections 7.3.5, 8.2.3 and 8.4.5] illustrate the use of CAM-C, and the commentary indicates that the process was relatively straightforward. In addition, the figures used in the CSM-C cells indicate the strength of the interface in an easily understandable way.

Subsidiary question 2. Can a new method be created to identify safety hazards that other methods detect understandably?

A comparison between CAM and two other methods in Chapter 7 [Section 7.4] compares CAM and two other methods. The results indicate that CAM performs at least as well as the other representative methods. However, it is acknowledged that this is a single case, and the results may differ with a different configuration. The analysis in Section 7.4 indicates that CAM may be a superior method because it captures data from a wide variety of sources and then reduces the data at the end to provide a focused answer, as described in Section 7.4.1 and illustrated in Figure 34. It would appear that this characteristic would give CAM a general advantage independent of the configuration of the system under consideration.

9.4 Weaknesses and shortcomings

The industry survey had 30 respondents. As reported in Chapter 4, this has affected the reliance placed on the results. The 90% selected confidence level signifies that the sample will remain within the calculated precision for the survey nine times out of ten. However, with 30 valid responses, the precision has dropped to 79%, indicating that the survey will not represent the population a fifth of the time. Consequently, while the survey is not definitive, it does provide indicators of industry trends. Therefore, in the event of an unrepresentative survey result, the insights fed into the development of CAM would be in error.

The research has provided a number of test cases to demonstrate the successful application of CAM and supported this with the theory, which provides a robust case for its use. However, it has essentially been conducted on an academic level. Accordingly, it has not had a great deal of direct input and feedback from the industry about the feasibility of CAM in the field. It might be that despite the hopes for widespread acceptance and use that there is little take-up as is the case with STAMP, reported in the survey in Chapter 4. Alternatively, to paraphrase Underwood and Waterson (2013b), it could be used in academia only. However, efforts have been made during this research to address issues that have arisen with other techniques such as complexity.

Given the numerous techniques that are claimed to exist, the research has only covered a selection. It has been influenced by the experiences and preferences of the Author. Accordingly, despite the Author's efforts, it is conceivable that an important technique was missed, which negates the need for CAM. Nevertheless, it is asserted by the Author that the research contained within this thesis contains an important contribution to the field of safety risk assessment.

The test cases are limited in depth and length by a lack of information and a limit on time available. Hence, they are, with the exception of Chapter 7, not fully-fledged case studies as described by the United States Audit Office (United States General Accounting Office, 1990). Therefore, because of the limitations, there is a risk that when applied to a full complex field study, the method does not scale up and is found, in practice, to be difficult to apply. The test cases are based on actual events, which, to a certain extent, provides a measure of mitigation. Furthermore, the scale of the examples has been large, providing a measure of assurance that CAM will scale up.

Test cases have been the main assurance strategy employed; these, by their nature, are only examples. They can only demonstrate that the technique works in that instance, and it cannot be inferred that the technique will work in all cases. This is the same for all prospective techniques because currently, there is no mathematical basis to prove safety in all but the most trivial cases. In effect, this is a case of the 'all swans are white' problem posed by Popper, as cited by Shearmur and Stokes (2016). It is impracticable to prove because all risk assessments in the world would have to be assessed. It is a weakness with the assurance strategy because it can only prove a negative and not a positive. That said, this test case method has been adopted by many other studies as a valid technique, cited by Rahim and Baksh (2003), for example. Consequently, it can only be stated that CAM has not failed with the examples used, but confidence can be drawn from the examples, which are typical cases in the rail industry.

It proved not to be practical to stage a workshop to pilot CAM with other practitioners due to the COVID-19 epidemic, and the practical demonstrations

remain the sole work of the Author. Consequently, the apparent clarity of the concepts to the Author may not transfer to other practitioners when they try and use CAM.

The test cases have used qualitative techniques throughout, primarily as a consequence of the limitations of the source data as well as personal preference. It means that a practical demonstration has not taken place for the use of CAM in a purely quantitative environment, although in theory, there is no foreseeable reason why it should not work. In some ways, the qualitative case is more complicated because enumerators are used in place of linear scalars.

There has been no demonstration of the conversion of the source data from different analysts into a single combinable entity, as described in Chapter 6. However, from a survey undertaken by Underwood and Waterson (2013a) it appears that this is not an unfamiliar practice. Therefore, it should not prove an insurmountable problem for CAM practitioners.

Only two subsystem analysis techniques have been used in the test cases, FMEA and the cause-consequence tables, and therefore, the compatibility of the other traditional techniques for use in CAM stage 2 have not been tested in practice. Conversely, from the Author's experience, there is no reason to believe that they will not be compatible and the level of difficulty align with the table provided in Section 6.3.8.

Finally, the testing in the thesis has covered a sample of the analysis domain specified by the CAM technique in Chapter 6 due to limitations of time and resource and the fact, that in theory, the domain is for practical purposes infinite.

Therefore, it is left for others to adopt CAM and apply it further to increase the breadth of experience.

9.5 Further work

This thesis has created initial research on CAM for others to take forward.

As explained in Section 9.4, only the Author has used CAM due to COVID. Further work is required to establish that CAM is understandable and usable by a general system safety community. For example, by holding a workshop of potential users to work through an example incident and using the feedback to further develop and refine CAM into a valuable assessment method.

Significantly, as identified in Chapter 8 [Section 8.3], training material needs to be developed so that others may become familiar with CAM and generate a user community. Increasing the community will assist in identifying errors and areas for improvement. In addition, the user instructions provided in Appendix J should be refined and checked for understandability. Furthermore, online training material should be developed from refined instructions.

The current work has been applied to problems where the answer is already known, i.e., RAIB reports. This prior knowledge, inevitably, will bias the application of the method, albeit subconsciously. Piloting CAM on a live project would provide additional assurance that it is a viable technique.

It would be a significant advance to apply the method to a large project in parallel with a more traditional approach to obtain contemporary proof to support the conclusions of this thesis.

Project or system complication is a relative term, with individuals having different views about what constitutes a complicated project based on experience. For example, some may view rail projects in the main as large but not necessarily complicated. Similarly, where projects mainly deal with earthworks and mechanical systems, they are unlikely to be complex. On the other hand, Thameslink was given as an example of a complex project in Chapter 1. In this case, the geographic spread and the interaction of the various parts of the infrastructure, trains and people at multiple points cause complexity. Still, others could be complex because of the technical systems involved, possibly involving interconnected signalling and communication systems, similar to the example of Chapter 8 [Section 8.4]. CAM development would benefit from more application to complicated and complex projects featuring the different causes of complexity mentioned to determine how well CAM can cope.

Currently, CAM addresses the issue of creating a risk assessment that indicates the acceptability of the level of risk as a result of controls (be they existing controls or mitigations). A further positive addition for CAM is to include an indication of the number of controls for each risk using the DMM principle. In this way, the 'strength' of the system could be graphically shown. Those places where a system is reliant on few controls could be highlighted as areas where strengthening may be required. Including this feature will require further work.

As previously described, the work documented in this thesis is only a sample of the potential risk analysis domain defined by the Author for CAM in Chapter 6, and further work will be required to explore this field in greater depth.

Furthermore, there is confidence that CAM is a generally applicable system safety risk analysis method, but currently, there is no evidence that this is the case.

Future work could include applying CAM to nuclear, aviation and defence industries. This work would provide evidence of CAM's general applicability.

9.6 CAM assessment

A reference set of criteria (from Chapter 6 Section 6.1) is utilised to assess whether CAM is an improvement over current risk analysis methods. In Table 73, three techniques are compared against the set of criteria. The three methods have been selected using the same criteria as was used to select them in Chapter 7 Section 7.4 as representative risk analysis methods. Each method has been allocated a grade by the Author for support of the criteria on the basis of the evidence indicated in the various sections of the thesis. These grades range from:

- Good meaning the criterion is well supported by the method,
- Average representing a state where there is some support and
- Poor indicating that there is little support.

Table 73 Comparison of selected risk assessment methods

Criterion	Risk assessment methods												Commentary
	CAM				STPA-STAMP				FMEA				
	Good	Average	Poor	Evidence (Section)	Good	Average	Poor	Evidence (Section)	Good	Average	Poor	Evidence (Section)	
Familiarity with technique		✓		6.3 7.3 8.2			✓	4.1	✓			4.1	CAM uses known methods in stage 2 and stage 5 which are familiar to safety practitioners, as described in Chapter 6. Therefore, there will be a measure of familiarity with part of the process.
Able to assess multiple connected systems	✓			7.3 8.2 8.4	✓			4.2			✓	4.1 4.2	
Able to analyse the physical system in detail	✓			7.3 8.2			✓	7.4	✓			4.2 7.4	
Flexibility in the analysis slant	✓			6.3			✓	7.4			✓	4.2	

		Risk assessment methods												
		CAM				STPA-STAMP				FMEA				
Criterion	Good	Average	Poor	Evidence (Section)	Good	Average	Poor	Evidence (Section)	Good	Average	Poor	Evidence (Section)	Commentary	
Analysis understandable	✓			6.3 7.3 8.2 8.4			✓	7.4		✓		4.2 7.4	For the FMEA, it is understandable as long as it addresses a single system and the table is reasonably small.	

CAM meets Underwood and Waterson (2013b) criteria for 'systems thinking' and 'useability' which are marks of a useful technique, as shown in Chapter 8, Section 8.3. In chapters 7 and 8, CAM met the satisfaction requirements of identifying the safety risks, being economical and applicable. In several cases, CAM identified additional risks missed by others. Table 73 indicates CAM performs better against the criteria than the other methods. Therefore, it seems, the Author's assessment indicates that CAM could be a significant improvement over current techniques, incorporating the best features of existing techniques (at the subsystem level). Moreover, CAM supplements these techniques with other processes to create a risk analysis method that provides a complete understandable system risk analysis. Concluding from the evidence available, there is a reasonable likelihood that **CAM could be better than existing techniques.**

9.7 Final conclusions

The thesis has shown there is justification for a new method, and the proposed method CAM is a suitable candidate to fill the gap in the modern railway environment, where subsystems are often combined by connecting through pervasive communication infrastructure.

The research question has been answered in-depth, as set out in Section 9.3 of this chapter. A literature review, survey, desktop data review has proven effective as a method of first justifying that a new method is required and then providing inputs to shape CAM. The tactic of using test cases has been successful by providing concrete assurance that CAM is a valid risk assessment method.

It has been demonstrated through the case study in Chapter 7 that CAM performs well when measured against other contemporary techniques. The case study indicates that CAM may have superior performance.

It is recognised, while progress has been made, not all aspirations envisioned at the start of the research have been met, where the objective was to create a fully-fledged method. Acknowledged weaknesses remain as described in Section 9.4, due in large part to limitations on data and resources. Further work has been identified in section 9.5, where it is hoped that others may fill the remaining gaps.

The research question has been positively answered by the content of the thesis and the proposed new analysis method CAM. This method is potentially capable of being applied to complex and complicated projects and providing an assessment of whether the attendant risks are acceptable. Furthermore, Section 9.6 has described how CAM could be a significant improvement on existing risk assessment methods.

Consequently, it is concluded that there is a need for CAM and that there is a reasonable likelihood that it could be better than those safety risk analysis methods in current use. Overall, it is further concluded that the research and, consequently, the thesis has been successful.

References

Adams, J. G. U. (1994) 'Seat belt legislation: Revisited.' *Safety Science*, 18 pp 135-152.

Aegis Engineering (2019) *Aegis Engineering Systems* Available at: <https://aegisengineering.co.uk/> (Accessed: 3/9/2019).

amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment 2015

Anleitner, M. A. (2010) *Power of Deduction : Failure Modes and Effects Analysis for Design*. Milwaukee: ASQ Quality Press.

Aven, T. (2008) *Risk Analysis : Assessing Uncertainties Beyond Expected Values and Probabilities*. Chichester: J Wiley & Sons.

Barnatt, N. (2016) *PhD proposal: A PhD research project on safety risk assessment of complex changes to railway infrastructure and vehicles*. Unpublished.

Barnatt, N. (2019a) *Initial survey development*. Unpublished.

Barnatt, N. (2019b) *Initial survey pilot report*. Unpublished.

Barnatt, N. and Jack, A. C. R. (2018) 'Safety analysis in a modern railway setting.' *Safety Science*, 110 pp 177-182.

Bayesia S.A.S (2020) *Bayesian Networks Representation of the Joint Probability Distribution* Available at: <https://www.bayesia.com/bayesian-networks-joint-probability-distribution> (Accessed: 27/05/2020).

Benner, L. (1985) 'Rating Accident Models and Investigation Methodologies.' *Journal of Safety Research*, 16 pp 105-126.

Bishop, P., G, Bloomfield, R., E and Froome, P., K, D (2001) *Justifying the use of software of uncertain pedigree (SOUP) in safety related applications*. Norwich: Health and Safety Executive.

Bonzo, S., M, McLain, D. and Avent, M., S (2016) 'Process Modeling in the Operating Room: A Socio-Technical Systems Perspective.' *Systems Engineering*, 19 pp 267-277.

Boulanger, J. (2014) *Formal Methods Applied to Industrial Complex Systems: Implementation of the B Method*. London: ISTE Ltd and John Wiley & Sons inc.

Bowman, C. (1990) *The Essence of Strategic Management*. London: Prentice Hall.

Branch, R. A. I. (2017) *Class investigation into accidents and near misses involving trains and track workers outside possessions*. Derby: Branch, R. A. I.

British Standards Institute (2010) *DD 261 Human reliability – Guide to the fundamental considerations* Milton Keynes: British Standards Institute.

CENELEC (1999) *EN 50126:1999 Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Basic requirements and generic process* Brussels: CENELEC.

CENELEC (2003) *EN 50129:2003 Railway Applications - Communication, Signalling and processing systems - safety related electronic systems for signalling* Brussels: CENELEC.

CENELEC (2006) *EN 60812:2006 Analysis techniques for system reliability — Procedure for failure mode and effects analysis (FMEA)* Brussels: CENELEC.

CENELEC (2011) *EN 50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems* Brussels: CENELEC.

CENELEC (2017) *EN 50126:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)* Brussels: CENELEC.

Common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009 2013

The Concise Oxford Dictionary of Current English. Sykes, J., B (ed.) (1979) Sixth Edition. Oxford: Clarendon Press,.

Cooper, M. D. (2022) 'The Emperor has no clothes: A critique of Safety-II.' *Safety Science*, 152 pp.

David Wilson Homes (2020) *David Wilson Homes@Mickleover* Available at: <https://www.dwh.co.uk/new-homes/city-of-derby/h723801-david-wilson-homes-@mickleover/> (Accessed: January 2020).

De Lessio, M. P., Cardin, M. A., Astaman, A. and Djie, V. (2015) 'Process to Analyze Strategic Design and Management Decisions Under Uncertainty in Complex Entrepreneurial Systems.' *Systems Engineering*, 18 pp 604-624.

Dekker, S. W. A. (2005) *Ten Questions About Human Error. A view of Human Factors and System Safety*. London: CRC Press LLC.

Dekker, S. W. A. (2006) *The Field Guide to Understanding Human Error*. Aldershot: Ashgate.

Dunleavy, P. (2003) *Authoring a PhD: how to plan, draft, write, and finish a doctoral thesis or dissertation*. Basingstoke: Palgrave Macmillan.

Dunsford, R. and Chatzimichailidou, M. (2020) 'Introducing a system theoretic framework for safety in the rail sector: supplementing CSM-RA with STPA.' *Safety and Reliability*, 39 pp 59-82.

Ed. Laylard, R. and Glaister, S. (1994) *Cost-Benefit Analysis*. Cambridge: Cambridge University Press.

Edwards, A. W. F. (1992) *Likelihood Expanded Edition*. London: The Johns Hopkins University Press.

Electrical and Mechanical Services Department (2019) *Investigation Report on Incident of the New Signalling System Testing on MTR Tsuen Wan Line*. Hong Kong: Department, E. a. M. S.

Electricity at Work Regulations 1989

Eppinger, S. D. and Browning, T. R. (2012) *Engineering Systems : Design Structure Matrix Methods and Applications*. London: MIT Press.

Fleming, C. (2013) *STPA Advanced Tutorial* Available at: http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/STPA_advanced_tutorial1.pdf (Accessed: 27/03/2020).

Fleming, C., H and Leveson, N., G (2016) 'Early Concept Development and Safety Analysis of Future Transportation Systems.' *IEEE Transactions On Intelligent Transportation Systems*, pp.

French, S., Bedford, T. and Atherton, E. (2005) 'Supporting ALARP decision making by cost benefit analysis and multiattribute utility theory.' *Journal of Risk Research*, 8 pp 207-223.

Grant, E., Salmon, P. M., Stevens, N. J., Goode, N. and Read, J. (2018) 'Back to the future: What do accident causation models tell us about accident prediction?'. *Safety Science*, 104 pp 99-109.

Haddon-Cave, C. Q. (2009) *AN INDEPENDENT REVIEW INTO THE BROADER ISSUES SURROUNDING THE LOSS OF THE RAF NIMROD MR2 AIRCRAFT XV230 IN AFGHANISTAN IN 2006*. London: Commons, H. o.

Health and Safety at Work Act 1974

Health and Safety Executive (2001) *Reducing risks, protecting people. HSE's decision making process*. Norwich: Health and Safety Executive,.

HM Treasury (2011) *The Green Book: Appraisal and Evaluation in Central Government*. London.

Hollnagel, E. (2012) *The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems*. Farnham Surrey UK: Ashgate Publishing Ltd.

House of Commons (2017) *Rail Sector Report* London: House of Commons.

IEEE (2011) *IEEE Recommended Practice for Functional Testing of a Communications-Based Train Control (CBTC) System* New York: IEE,.

INCOSE (2015) *Systems Engineering Handbook : A Guide for System Lifecycle Processes and Activities*. Hoboken, New Jersey, United States of America: Wiley.

Institute of Railway Signalling Engineers (2005) *British Railway Signalling Practice - Interlocking Principles & Systems*. London: Institute of Railway Signalling Engineers.

International Electrotechnical Commission (2001) *BSIEC 61882:2001 HAZARD AND OPERABILITY STUDIES (HAZOP STUDIES) – APPLICATION GUIDE* Geneva: International Electrotechnical Commission.

International Standardization Organization (2015) *ISO/IEEE 15288:2015 Systems and Software Lifecycle Process* Geneva: International Standardization Organization.

Jarzębowicz, A. and Wardziński, A. (2015) 'Integrating confidence and assurance arguments', *System Safety and Cyber Security 2015*, Bristol The IET.

Jones-Lee, M., Loomes, G., Spackman, M., Sugden, R. and Thomson, T. (2006) *T430: The Definition of VPF and the Impact of Societal Concerns*. London: Board, R. S. a. S.

Kahneman, D. (2011) *Thinking, Fast and Slow*. London: Penguin Books.

Kamensky, J. (2011) 'Managing the Complicated vs. the Complex' The Business of Government fall/winter 2011 Available at: <http://www.businessofgovernment.org/sites/default/files/JohnKamensky.pdf> (Accessed: 12/04/2021).

Kasunic, M. (2005) *Designing an Effective Survey*. Pittsburgh, Pennsylvania USA.

Kim, D. S. and Yoon, W. C. (2013) 'An accident causation model for the railway industry: Application of the model to 80 rail accident investigation reports from the UK.' *Safety Science*, 60 pp 57-68.

Krzanowski, W. J. (1998) *An Introduction to Statistical Modelling*. London: Arnold.

Le Coze, J. C. (2022) 'The 'new view' of human error. Origins, ambiguities, successes and critiques.' *Safety Science*, 154 pp.

Lepmets, M. (2017) *What is FMEA and how is it different from Hazard Analysis?* Available at: <https://softcomply.com/what-is-fmea-and-how-is-it-different-from-hazard-analysis/> (Accessed: 26/4/2020).

Leven, R. i. and Rubin, D. S. (1998) *Seventh Edition Statistics for Management*. London: Prentice-Hall International.

Leveson, N., G (2011) *Engineering a Safer World : Systems Thinking Applied to Safety*. Available at: <https://mitpress.mit.edu/books/engineering-safer-world> (Downloaded: 15/08/2019).

Leveson, N. G. (2016) *Introduction to: Systems Theoretic Accident Model & Processes (STAMP) WEBINAR REPLAY* Whiteley-Safety Available at: <https://www.youtube.com/watch?v=8bzWvII9OD4> (Accessed: 20/8/2017).

Leveson, N. G. and Thomas, J. P. (2018a) 'How to Do a Basic STPA Analysis', in *STPA Handbook* Cambridge, Massachusetts, USA:MIT, pp. 14-53 Available at: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf (Accessed: 27/03/2020).

Leveson, N. G. and Thomas, J. P. (2018b) *STPA Handbook*. Available at: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf (Downloaded: 27/03/20).

Lobo, J. P., Charchalakis, P. and Stipidis, E. (2015) 'Safety and security aware framework for the development of feedback control systems', System Safety and Cyber Security 2015, Bristol 21-22 October 2015. London: The IET.

Manson, S. M. (2001) 'Simplifying complexity: a review of complexity theory.' *Geoforum*, 32 pp 405-414.

Marsh, D. W. R. and Bearfield, G. (2008) 'Generalizing event trees using Bayesian networks.' *Journal of Risk and Reliability*, 222 pp 105-114.

Marshall, P., Hirmas, A. and Singer, M. (2018) 'Heinrich's pyramid and occupational safety: A statistical validation methodology.' *Safety Science*, 101 pp 180-189.

McCormack, B. and Hill, E. (1997) *Conducting a Survey The SPSS Workbook*. London: Thompson Business Press.

McGee, P. J. and Knight, J. C. (2015) 'Expert judgment in assurance cases', System Safety and Cyber Security 2015, Bristol 21-22 October 2015. London: The IET.

Miller v Secretary of State for Exiting the European Union. (2017): Supreme Court.

Ministry of Defence (2007) *Safety Management Requirements for Defence Systems* London:

Mohr, R. (2002) *Failure Modes and Effects Analysis* University of Wisconsin-Madison Available at: https://icecube.wisc.edu/~kitamura/NK/Flasher_Board/Useful/FMEA.pdf (Accessed: 08/05/2020).

Network Rail (2016) *Electrification* Available at: <http://www.networkrail.co.uk/asp/12273.aspx> (Accessed: 6/12/2016).

Network Rail (2018) *STE/HSMS/001 version 4.5 Network Rail (infrastructure) Ltd, Health & Safety Management System* Milton Keynes: Network Rail.

O'Neill, B. and Williams, A. (1998) 'Risk Homeostasis hypothesis: a rebuttal.' *Injury Prevention*, 4 pp 92-93.

Office of Rail and Road (2018) *Common Safety Method for Risk Evaluation and Assessment Guidance on the application of Commission Regulation (EU) 402/2013*. London: Office of Rail and Road.

Parmar, J. C. and Lees, F. P. (1987) 'The Propagation of Faults in Process Plants: Hazard Identification.' *Reliability Engineering*, 17 pp 277-302.

Pawitan, Y. (2001) *In All Likelihood*. Oxford: Clarendon Press.

Pearl, J. (1990) 'Reasoning with Belief Functions and Analysis of Compatibility.' *International Journal of Approximate Reasoning*, 4 pp 363-389.

Posey, C. A. (2012) *Under the Eurofighter's Hood Europe's frontline fighter is a marvel of technology*. Available at: <https://www.airspacemag.com/military-aviation/under-the-eurofighters-hood-100269558/> (Accessed: 28/8/2018).

Rahim, A. R. A. and Baksh, M. S. N. (2003) 'Case study method for product development in engineer-to-order organizations.' *Work Study*, 52 pp 25-36.

Rail Accident Investigation Branch (2011) *Derailment at Grayrigg 23 February 2007*. Derby: Rail Accident Investigation Branch.

Rail Accident Investigation Branch (2014) *RAIB's response to accident and incident notification* Available at: <https://www.gov.uk/guidance/raibs-response-to-accident-and-incident-notification> (Accessed: 24/03/20).

Rail Accident Investigation Branch (2017) *Trains passed over washed out track at Baildon, West Yorkshire 7 June 2016*. Derby: Rail Accident Investigation Branch.

Rail Accident Investigation Branch (2018a) *Collision at London Waterloo 15 August 2017*. Derby: Rail Accident Investigation Branch.

Rail Accident Investigation Branch (2018b) *Overtaking of a tram at Sandilands junction, Croydon 9 November 2016*. Derby: Rail Accident Investigation Branch.

Rail Accident Investigation Branch (2020) *Passenger train derailment near Carmont – updated 21/08/2020* Available at: <https://www.gov.uk/government/news/passenger-train-derailment-near-carmont-updated-21082020> (Accessed: 2/09/2020).

Rail Safety and Standards Board (2007) *Engineering Safety Management (The Yellow Book) Volumes 1 and 2 Fundamentals and Guidance*. 4. London: Rail Safety and Standards Board,.

Rail Safety and Standards Board (2014a) *Guidance on the use of cost-benefit analysis when determining whether a measure is necessary to ensure safety so far as is reasonably practicable*. London: Rail Safety and Standards Board.

Rail Safety and Standards Board (2014b) *Safety Risk Model: Risk Profile Bulletin, version 8.1*. London: Board, R. S. a. S.

Rail Safety and Standards Board (2014c) *Taking Safe Decisions: How Britain's railways take decisions that affect safety*. London: Board, R. S. a. S.

Rail Safety and Standards Board (2017) *10 years after Grayrigg, rail passengers are safer than ever* Available at: <https://www.rssb.co.uk/News/Pages/10-years-after-grayrigg-rail-passengers-are-safer-than-ever.aspx> (Accessed: 28/5/17).

Rail Safety and Standards Board (2019) *Taking Safe Decisions - Safety-Related CBA* Available at: <https://www.rssb.co.uk/Standards-and-Safety/Improving-Safety-Health--Wellbeing/Applying-Guidance-and-Good-Practice/Taking-Safe-Decisions/Taking-Safe-Decisions-safety-related-CBA> (Accessed: 06/05/2020).

The Railways (Interoperability) Regulations 2011 2011

The Railways and Other Guided Transport Systems (Safety) Regulations 2006 2006

Rasmussen, J. (1997) 'Risk Management in a Dynamic Society: A Modelling Problem.' *Safety Science*, 27 pp 183-213.

Reason, J. (1997) *Managing the Risks of Organizational Accidents*. Aldershot: Ashgate.

Reason, J. (2016) *Organizational Accidents Revisited*. Farnham Surrey UK: Ashgate.

Reason, J., Hollnagel, E. and Paries, J. (2006) *Revisiting the Swiss Cheese Model of Accidents*. Bretigny-Sur-Orge, France: European Organisation for the Safety of Air Navigation.

Ricardo Rail (2019) *Rail* Available at: <https://rail.ricardo.com/our-regions/uk> (Accessed: 3/9/2019).

Salmon, P. M., Cornelissen, M. and Trotter, M. J. (2012) 'Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP.' *Safety Science*, 50 pp 1158-1170.

Salmon, P. M., Walker, G. H. and Stanton, N. A. (2015) 'Broken components versus broken systems: why it is systems not people that lose situation awareness.' *Cognition & Work*, 17 pp 179-183.

Sanford, A. and Moosa, I. (2012) 'A Bayesian network structure for operational risk modelling in structured finance operations.' *The Journal of the Operational Research Society*, 63 pp 431-444.

Sargut, G. and McGrath, R. (2011) 'Learning To Live with Complexity.' *Harvard Business Review*, 89 pp 68-76.

Shafer, G. (1976) *A Mathematical Theory of Evidence*. London: Princeton University Press.

Shearmur, J. and Stokes, G. (ed.) (2016) *The Cambridge Companion to POPPER*. Cambridge: Cambridge University Press.

Sieker, B., M (2015) 'A Proposal for Improving the Applicability of Formal Methods in the Functional Safety Base Standard IEC 61508-3', System Safety and Cyber Security 2015, Bristol 21-22 October 2015. London: The IET.

Simmons, A. (2015) 'Presidential Address: Moving to a Data Enabled Railway', IRSE News May 2015 pp. 2-4.

Svedung, I. and Rasmussen, J. (2002) 'Graphical representation of accident mapping scenarios: mapping system structure and the causation of accidents.' *Safety Science*, 40 pp 397-417.

SWARB (2016) *Edwards v National Coal Board; CA 1949* Available at: <http://swarb.co.uk/edwards-v-national-coal-board-ca-1949/> (Accessed: 6 December 2016).

SWARB (2018) *Health and Safety - From: 1930 To: 1959* Available at: <https://swarb.co.uk/lisc/HltSf19301959.php> (Accessed: 20/02/2020).

Teegavarapu, S. and Summers, J. (2008) *ASME 2008 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference*. 3-6 August 2008 New York. New York: 2008.

Thales Group (2015) *Communication Based Train Control Systems* Available at: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=18&cad=rja&uact=8&ved=2ahUKEwiF75iT1_DjAhWzunEKHe6XApkQFjARegQICBAC&url=http%3A%2F%2Fwww.irsteindia.com%2Fpresentations-august2015%2FIRSE-Seminar-V3.pptx&usq=AOvVaw2MpxV6IT3wxhF25VUJ4du6 (Accessed: 7/8/19).

The Open University (No Date) *5.4 Methodology, method, technique, and tools* Available at: <https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/managing-complexity-systems-approach-introduction/content-section-15.4> (Accessed: 7/10/19).

Thigle, V. (2013) *What is the relationship between pressure differential and the amount of fluid that flows through a pipe?* Available at: <https://www.quora.com/What-is-the->

[relationship-between-pressure-differential-and-the-amount-of-fluid-that-flows-through-a-pipe](#) (Accessed: 20/04/2019).

Thomas, J. (2013) *Basic STPA Tutorial* Available at: http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/Basic_STPA_Tutorial1.pdf (Accessed: 27/03/2020).

Turner, S., Keeley, D., Glossop, M. and Brownless, G. (2002) *Review of Railway Safety's Safety Risk Model*. Sheffield: Laboratory, H. a. S.

Underwood, P. and Waterson, P. (2013a) 'Systemic accident analysis: Examining the gap between research and practice.'*Accident Analysis & Prevention*, 55 pp 154-164.

Underwood, P. and Waterson, P. (2013b) 'Systems thinking, the Swiss Cheese Model and accident analysis:A comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap and STAMP models.'*Accident Analysis & Prevention*, 68 pp 75-94.

United States General Accounting Office (1990) *Case Study Evaluations*. Washington DC: Office, U. S. G. A.

University of Calgary (unknown) Critical Values for the Wilcoxon Signed-Rank Test [table]. Available at: https://science.ucalgary.ca/sites/default/files/teams/7/wilcoxon_signed_rank_table.pdf (Accessed: 4/9/2019).

Van Gulijk, C., Hughes, P., Figueres-Esteban, M., Dacre, M. and Harrison, C. (2015) 'Big Data Risk Analysis for Rail Safety? In: Safety and Reliability of Complex Engineered Systems', ESREL 2015, Zurich Huddersfield: Huddersfield University.

Whittingham, R. B. (2004) *The Blame Machine: why human error causes accidents*. London: Elsevier Butterworth Heinemann.

Wilde, G. J. S. (1998) 'Risk homeostasis theory: An overivew.'*Injury Prevention*, 4 pp 89-91.

Woods, D. D. (2018) 'The theory of graceful extensibility: basic rules that govern adaptive systems.'*Environment Systems and Decisions*, 38 pp 433–457.

Zhou, Y. and Yan, F. (2018) 'Causal Analysis to a Subway Accident: A Comparison of STAMP and RAIB.'*MATEC Web of Conferences*, 160 pp not numbered.

Appendix A - Industry risk analysis survey invitation and questions

Invitation sent to respondents:

Dear Colleague,

Link to survey <https://www.surveymonkey.co.uk/r/VHGZJ88>

The survey is open until midnight 4 August 2019

A PhD research project is underway to understand the use of system safety risk analysis techniques in the railway industry in Great Britain. The objective of the project is to increase the efficiency, improve and simplify risk analysis within the railway industry. This survey has been created to gather data to understand the current knowledge of and use of techniques in risk analysis and assessment. You and your employees' input will provide valuable data which will be collated and analysed with other responses. The survey should take a maximum of 10 minutes. All the data collected will be anonymised, and only aggregate data will be subject to further analysis and publication.

Your help is requested to:

- a) Complete a questionnaire, if you deal with any aspect of safety assessment yourself;
and
- b) allow and encourage your employees to complete the attached survey. It would be of great help if you could distribute the attached survey (link) to up to 30 of your employees who perform roles of either:
 - Safety engineers
 - Project managers
 - Designers
 - Assessor contractors
 - Safety decision makers

Thank you for your valuable help.

Neil Barnatt

PhD Post graduate research student University of Birmingham



Introductory message from the surveyMonkey site landing page

Welcome to the safety risk analysis research survey

Welcome to this safety risk analysis survey and thank you for taking part. The survey should take no more than 10 minutes. All the data collected will be anonymised, and only aggregate data will be subject to further analysis and publication.

A research project is underway to understand the use of risk analysis techniques in the railway industry in Great Britain. This survey has been created to gather data to understand the current knowledge of and use of techniques in risk analysis and assessment. Your input will provide valuable data which will be collated and analysed with other responses. By completing this survey, you will be agreeing to the use of the data for the purposes of the research outlined. A link to the summarised anonymised survey data can be provided on written request when completed.

Once submitted it will not be possible to extract or delete the data from the survey due to the anonymous nature of the data handling of the survey tool.

(The survey will close at midnight 4 August 2019)

Thank you for participating in the survey. Your feedback is valued and important.

Neil Barnatt

PhD Post graduate research student University of Birmingham

NJB619@student.bham.ac.uk

Questions

1. Please indicate which area of the industry you operate in (select the option which represents you best)

- | | |
|---|---|
| <input type="radio"/> Mainline Infrastructure manager | <input type="radio"/> Equipment supplier |
| <input type="radio"/> TOC | <input type="radio"/> Service/design consultancy |
| <input type="radio"/> HS2 | <input type="radio"/> Risk assessment consultancy |
| <input type="radio"/> ROSCO | <input type="radio"/> Not listed |
| <input type="radio"/> Vehicle supplier/manufacturere | |

2. Please indicate the type of activity undertaken by you

- | | |
|---|---|
| <input type="radio"/> Upgrade | <input type="radio"/> Maintenance |
| <input type="radio"/> Development | <input type="radio"/> Operation |
| <input type="radio"/> New product development | <input type="radio"/> Risk assessment service |
| <input type="radio"/> Product supply | <input type="radio"/> Not listed |
| <input type="radio"/> Renewal | |

3. Please indicate your level of understanding of the following risk assessment techniques

	None	Aware	Basic	Proficient	Advanced	Expert
Historical data analysis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Visual data mapping	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hazard identification prompt lists	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Risk control prompts	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Structured What If Technique (SWIFT)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hazard Log	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Task Based Risk Assessments	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interviews	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hierarchical Task Analysis (HTA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hazard and Operability Study (HazOP)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fault Tree Analysis (FTA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

	None	Aware	Basic	Proficient	Advanced	Expert
Event Tree Analysis (ETA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cause consequence analysis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Common consequence tool	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Failure Modes and Effects Analysis (FMEA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bow Tie Analysis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Failure Modes and Effects and Criticality Analysis (FMECA)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
STAMP	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Swiss Cheese Model	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Formal methods	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Code of Practice compliance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reference system comparison	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Functional Resonance Analysis Method (FRAM)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. Please select and rank the risk analysis techniques used by you or know to be used by your team in order of preference of use (1 being the most preferred technique)

<input type="text"/>	Historical data analysis	<input type="checkbox"/> Not used
<input type="text"/>	Visual data mapping	<input type="checkbox"/> Not used
<input type="text"/>	Hazard identification prompt lists	<input type="checkbox"/> Not used
<input type="text"/>	Risk control prompts	<input type="checkbox"/> Not used
<input type="text"/>	SWIFT	<input type="checkbox"/> Not used

<input type="checkbox"/> Hazard Log	<input type="checkbox"/> Not used
<input type="checkbox"/> Task Based Risk Assessments	<input type="checkbox"/> Not used
<input type="checkbox"/> Interviews	<input type="checkbox"/> Not used
<input type="checkbox"/> Hierarchical Task Analysis (HTA)	<input type="checkbox"/> Not used
<input type="checkbox"/> HazOP	<input type="checkbox"/> Not used
<input type="checkbox"/> Fault Tree Analysis (FTA)	<input type="checkbox"/> Not used
<input type="checkbox"/> Event Tree Analysis (ETA)	<input type="checkbox"/> Not used
<input type="checkbox"/> Cause consequence analysis	<input type="checkbox"/> Not used
<input type="checkbox"/> Common consequence tool	<input type="checkbox"/> Not used
<input type="checkbox"/> FMEA	<input type="checkbox"/> Not used
<input type="checkbox"/> Bow Tie Analysis	<input type="checkbox"/> Not used
<input type="checkbox"/> FMECA	<input type="checkbox"/> Not used
<input type="checkbox"/> STAMP	<input type="checkbox"/> Not used
<input type="checkbox"/> Swiss Cheese Model	<input type="checkbox"/> Not used
<input type="checkbox"/> Formal methods	<input type="checkbox"/> Not used

Code of Practice compliance

Not
used

Reference system comparison

Not
used

Functional Resonance Analysis Method (FRAM)

Not
used

5. Please indicate what part of the risk assessment process you consider the following techniques cover
(select the columns you consider apply)

	Identification	Analysis	Evaluation	Recording	Risk treatment
Historical data analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Visual data mapping	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hazard identification prompt lists	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Risk control prompts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SWIFT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hazard Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Task Based Risk Assessments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Interviews	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hierarchical Task Analysis (HTA)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HazOP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fault Tree Analysis (FTA)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Event Tree Analysis (ETA)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cause consequence analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Common consequence tool	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FMEA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bow Tie Analysis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FMECA	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
STAMP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Swiss Cheese Model	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Formal methods	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Code of Practice compliance	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reference system comparison	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Functional Resonance Analysis Method (FRAM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6. Please indicate by selecting where on the scale below how often you and or your team risk assess equipment and or operational processes prior to integration into the operational railway or as part of integration or post integration into the operational railway.

	None	Rarely	Sometimes	Often	Always
Pre-integration risk assessment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Integration risk assessment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Post integration risk assessment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. Please indicate on the scale provided when assessing risks to what extent do you consider the changed items only or a take a wider view including the general environment

changed items only	No preference	wider view including the general environment
<input type="radio"/>		<input type="checkbox"/>

8. When assessing risk does your team take account of the existing equipment or processes and environment in a specific target environment or is the analysis undertaken in a virtual setting with no specific target environment

- Specific target
- No specific target (virtual)

9. Please indicate on the scale provided to what extent when assessing a whole complex system do your team analyse the system as a whole or by parts

- Over 75% by parts
- Between 60% and 75% as an integrated whole
- Between 60% and 75% by parts
- Over 75% as an integrated whole
- A mixture of parts and an integrated whole between 50% and 59%

10. Please indicate the level of alignment of the risk acceptance criteria listed, with the assessment strategy taken and risk assessment methods used by you and your team

	Strongly aligns	Partially aligns	Unsure	Little alignment	Not at all
Better than current level of risk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Equivalent to the current level of risk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A level of risk that is As Low As Reasonably Practicable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Meets prescribed target level of risk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
A level of risk that is As Low As Practicable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Appendix B - RAIB GB heavy rail accident report extracts analysis

The report index identified in the Report title column of the following table has been extracted from RAIB heavy rail accident reports

Table 74 RAIB GB heavy rail accident report extracts analysis reformulated RAIB data

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
Report 19/2016: Overspeed incident at Queen's Park	The driver manager who was being assessed did not slow the train for the emergency speed restriction as he had misunderstood details of the restriction given in an email. The assessing driver manager's knowledge of the emergency speed restriction was insufficient to notice the driver's error.	Yes	No	No	No	Yes	No	No	Yes	No	No	No	No
Report 21/2016: Collision at Barrow-upon-Soar	A passenger train collided with a conveyor boom projecting from an aggregates train standing in sidings.	No	Yes	No	No	Yes	No	No	Yes	No	Yes	Yes	No
Report 22/2016: Structural failure at Lamington viaduct	subsidence of Lamington viaduct resulted in serious deformation of the track as the passenger service passed over at a speed of about 110 mph (177 km/h). the viaduct's central river pier had been partially undermined by scour following high river flow	No	Yes	No	No	No	Yes	No	No	No	Yes	No	Yes

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
Report 23/2016: Fatal accident at Grimston Lane level crossing	A pedestrian was struck and fatally injured by a train on Grimston Lane footpath level	No	No	No	Yes	Yes	No	No	Yes	No	No	No	No
Report 01/2017: Occupied wheelchair contacting passing train, Twyford	A wheelchair occupied by a teenage girl moved towards the edge of platform 4 at Twyford station and came into multiple glancing contacts with the wagons of a passing freight train.	Yes	No	No	Yes	Yes	No	No	No	No	No	No	Yes
Report 02/2017: Collision at Plymouth station	A passenger train service collided with an empty train which was already waiting in the platform	Yes	No	No	No	Yes	No	No	Yes	No	No	No	No
Report 03/2017: Trains passed over washed out track at Baildon	Three passenger trains passed over a section of the single line at Baildon, where part of the supporting embankment had been washed away by flood water.	No	Yes	No	No	No	Yes	No	No	No	Yes	Yes	No
Report 04/2017: Collision at Hockham Road user worked crossing, Thetford	a passenger train collided with an agricultural tractor and trailer on a level crossing	No	Yes	No	Yes	Yes	No	No	Yes	No	No	Yes	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
Report 05/2017: Near miss between a train and a track worker, Shawford	A train travelling at about 85 mph (137 km/h) narrowly missed striking a track worker	No	No	Yes	No	Yes	No	No	Yes	No	No	No	No
Report 07/2017: Track workers class investigation	The Rail Accident Investigation Branch (RAIB) has investigated a number of accidents involving track workers on Network Rail's infrastructure and has identified track worker safety as an area of particular concern	No	No	Yes	No	Yes	No	No	Yes	No	No	No	No
Report 08/2017: Near miss at Dock Lane level crossing	The passenger of a car that was waiting to cross the line was opening the gates at Dock Lane user worked crossing, when a train passed over the crossing. The signaller had given permission for the car to cross the line.	No	No	No	Yes	Yes	No	No	Yes	No	No	Yes	No
Report 09/2017: Fatal accident, Balham	a passenger, travelling on a Gatwick Express service suffered fatal injuries as a result of having his head out of a window and striking it on a signal gantry near	Yes	No	No	Yes	Yes	No	No	Yes	No	No	No	No
Report 10/2017: Partial collapse of a bridge onto open railway lines at Barrow upon Soar	a bridge carrying Grove Lane in Barrow upon Soar, Leicestershire, over the Midland Main Line, partially collapsed and a large volume of masonry fell onto the railway lines below. At the time of the collapse, core sampling work was being undertaken to investigate localised subsidence in	No	Yes	No	No	No	No	Yes	No	No	Yes	No	Yes

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
	the footpath on the south side of the bridge. The bridge was closed to the public when the collapse occurred, but the railway lines below were open to traffic.												
Report 11/2017: Derailment and subsequent collision at Watford	a London-bound passenger train operated by London Midland struck a landslip at the entrance to Watford slow lines tunnel. The leading coach of the 8-car train derailed	No	Yes	No	No	No	Yes	No	No	No	Yes	No	Yes
Report 14/2017: Fatal accident at Alice Holt footpath crossing, Hampshire	a mobility scooter was struck by a train, and the scooter user fatally injured, at Alice Holt footpath crossing, Bentley, Hampshire.	No	No	No	Yes	Yes	No	No	Yes	No	No	No	No
Report 15/2017: Serious irregularity at Cardiff East Junction	Extensive resignalling and track remodelling work in and around Cardiff Central station. The driver, noticed that points in the route his train was about to take were not set in the correct position. The points had been left in this unsafe condition	No	Yes	No	No	No	No	Yes	Yes	No	No	No	No
Report 16/2017: Track worker near miss incidents at	The incidents occurred because the signaller authorised track workers to go onto a line over which he had just routed a train, having	No	No	Yes	No	Yes	No	No	Yes	No	No	No	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
Camden Junction South	overlooked the fact that engineering work was taking place on that line.												
Report 17/2017: Partial collapse of a wall onto open railway lines, Liverpool	Part of a wall at the top of a cutting 20 metres above the four track railway line between Liverpool Lime Street and Edge Hill stations, collapsed. Around 170 tonnes of masonry and other debris fell into the cutting in at least two separate falls	No	Yes	No	No	No	Yes	No	No	No	Yes	No	Yes
Report 19/2017: Freight train derailment at East Somerset Junction	Six wagons of a freight train carrying aggregates from Merehead Quarry to Acton Yard derailed at East Somerset Junction, between Westbury and Castle Cary. The accident blocked the Up Westbury line, and the train stopped when the brakes applied	No	Yes	No	No	No	Yes	No	No	No	No	Yes	No
Report 01/2018: Runaway of a maintenance train near Markinch	At about 04:25 hrs on Tuesday 17 October 2017, a maintenance train that was clearing leaf debris from the track, hit a tree just north of Markinch station, Fife. The debris from the tree disabled the train's braking system.	Yes	No	No	No	Yes	No	No	No	No	Yes	No	Yes
Report 03/2018: Trailer runaway near Hope, Derbyshire	At around 06:30 hrs on Sunday 28 May 2017, a trailer, being propelled by a small rail tractor between Edale and Bamford, became detached and ran away for a distance of around 1 mile (1.6	Yes	No	Yes	No	Yes	No	No	Yes	No	No	Yes	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
	km). It came to a stop at a set of points at Earles Sidings, near Hope. There were no injuries that required medical attention, and there was no significant damage to the infrastructure, the trailer or the tractor.												
Report 04/2018: Freight train derailment at Lewisham	Two wagons within an aggregate train derailed on newly-laid track at Courthill Loop South Junction in Lewisham, south-east London. The first of the wagons ran derailed	No	Yes	No	No	No	No	Yes	No	No	Yes	Yes	No
Report 05/2018: Explosion inside an underframe equipment case at Guildford	The explosion resulted in debris being ejected onto other platforms and a car park near the station. There were no injuries to passengers or staff. There was damage to the train, and to station furniture.	Yes	No	No	No	No	No	Yes	No	Yes	No	No	No
Report 06/2018: Passengers struck by a flying cable at Abergavenny (Y Fenni) station	A cable drooping from the station footbridge became caught on the train's roof. The train dragged the cable and caused it to be pulled from the footbridge until its end broke free from a distribution cabinet. Once free, the end of the cable struck a group of passengers on the footbridge stairs and caused minor injuries to three of them.	No	Yes	No	Yes	No	Yes	No	No	Yes	No	No	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
Report 07/2018: Fatal accident at Trenos footpath crossing near Llanharan	A pedestrian was struck and fatally injured by a train travelling from Cheltenham Spa to Maesteg, at Trenos footpath crossing near Llanharan, Rhondda Cynon Taf, South Wales. The pedestrian had walked onto the crossing	No	No	No	Yes	Yes	No	No	Yes	No	No	No	No
Report 08/2018: Collision at Stainforth Road level crossing	A car collided with the rear-most wagon of a stationary freight train at Stainforth Road Automatic Half-Barrier level crossing, near Doncaster. The crossing's warning equipment was not operating and its half-barriers were raised when the car approached and entered the crossing. The car driver was not alerted to the presence of the train by the crossing's warning devices because the design of the level crossing's control circuits had permitted it to re-open to road traffic while it was still occupied by the train.	No	Yes	No	Yes	Yes	No	No	No	No	No	Yes	No
Report 09/2018: Freight train derailment at Ely West Junction	The rear 12 wagons of a freight train carrying containers derailed at Ely West Junction on the line between Ely and March. The train was travelling at 41 mph (66 km/h) at the time of the derailment. It ran derailed for approximately 350 metres, causing significant damage to the infrastructure.	Yes	No	No	No	No	Yes	No	No	Yes	No	No	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
	The first wagon to derail was an FEA-A wagon fitted with Y33 bogies. The derailment occurred because the damping on the bogies of this wagon was ineffective. The damping had become ineffective because the damping components, which had been on the wagon since it was built in 2003, had been managed to incorrect maintenance limits.												
Report 10/2018: Landslip and derailment at Loch Eilt, north-west Scotland	A large landslip on a remote section of line near Glenfinnan. The leading coach of the 2-car train derailed to the left and came to a halt embedded in landslip debris. The landslip originated from a natural hillside above the railway and was triggered by a combination of rainfall and snow melting during a rapid thaw. The ground may have been saturated before it froze. A protective fence, which had previously been installed near the railway to trap falling rocks was overwhelmed by the event	No	Yes	No	No	Yes	No	No	No	No	Yes	No	Yes
Report 11/2018: Near miss with a group of track workers at Egmonton level	A group of track workers narrowly avoided being struck by a train close to Egmonton level crossing, between Newark North Gate and Retford on the East Coast Main Line. A high speed passenger train was approaching the level	No	No	Yes	No	Yes	No	No	Yes	No	No	No	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
crossing, Nottinghamshire	crossing on the Down Main line at the maximum permitted line speed of 125 mph (201 km/h)												
Report 12/2018: Collision at Frogna Farm User Worked Crossing	A passenger train collided with a parcel delivery van at Frogna Farm user worked level crossing, near Teynham, in Kent. The train was travelling at 89 mph (143 km/h). It did not derail, and no-one on the train was hurt, but the train was damaged by the impact. The van was severely damaged and the van driver suffered serious injuries	No	No	No	Yes	Yes	No	No	Yes	No	No	No	No
Report 16/2018: Detrainment of passengers onto electrically live track near Peckham Rye station	<p>A London Overground service came to a stand shortly before reaching Peckham Rye station. A faulty component on the train had caused the brakes to apply, and the driver was unable to release them. There were about 450 passengers on the train.</p> <p>The train driver spoke over the railway radio system to the service controller, train technicians, and the signaller. Following these conversations he began, with the assistance of a member of staff from Peckham Rye station, to evacuate the passengers from the train via the door at the right-hand side of the driver's cab at the front of the train. This involved passengers climbing down vertical steps to ground level, very close to the live electric conductor rail (third rail) and walking</p>	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	Yes	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
	along the side of the line for about 30 metres to Peckham Rye station												
Report 17/2018: Extensive track damage between Ferryside and Llangennech, Carmarthenshire	Train 6B13, which was carrying oil-based products from Robeston oil terminal, Milford Haven, to Westerleigh oil terminal, Bristol, caused extensive damage to railway infrastructure over approximately 25 miles (40 km). After the train had been stopped, at the entrance to Llangyfelach Tunnel near Swansea, the driver found that there had been a catastrophic failure of the braking system on one of the fully laden wagons.	Yes	No	No	No	Yes	No	No	No	Yes	No	No	No
Report 19/2018: Collision at London Waterloo	A passenger train was leaving London Waterloo station when it collided with a stationary engineering train at a speed of 13 mph (21 km/h). No injuries were reported but both trains were damaged and there was serious disruption to train services until the middle of the following day	No	Yes	No	No	No	No	Yes	Yes	No	No	No	No
Report 20/2018: Near miss with track workers and trolleys at South Hampstead, London	A group of track workers narrowly avoided being struck by a train while placing trolleys on the track alongside South Hampstead station, north London. The train was travelling at 49 mph (79 km/h) towards London Euston station when the driver saw the group, sounded his horn and applied the brake. Three other members of the	No	No	Yes	No	No	Yes	No	Yes	No	No	No	No

RAIB Accident report		Cause based on		People affected		Source of incident			Type of incident				
Report title	Extracted summary	Train	Infrastructure	Track worker involvement	Member of the public injured	Operational	Maintenance	Construction	Human Error	Component failure	Subsystem failure	Multisystem event	Environmental effect
	work group, who were around 100 metres away from the staff placing the trolleys on the track, saw the train seconds earlier and shouted a warning to their colleagues who managed to remove the trolleys and get clear around two seconds before the train passed. One member of the group received a minor injury and many were distressed												
Report 01/2019: Runaway of a road-rail vehicle at Bradford Interchange	<p>At about 01:40 hrs on Friday 8 June 2018, a road-rail vehicle (RRV) ran away while being on-tracked at a road-rail access point south of Bradford Interchange station. The RRV ran downhill for approximately 340 metres, before coming to a stop as the track levelled out in the station. The RRV's machine operator and machine controller were able to run along with it and warned a member of track maintenance staff, who was able to move clear in time.</p> <p>The RRV ran away because its rail wheels were, incorrectly, partially deployed and because the rail wheel braking system had not been correctly maintained</p>	No	No	No	No	No	Yes	No	Yes	No	Yes	No	No

Appendix C - Rationalisation path example particulars

This appendix contains a non-railway example which has been used to develop CAM. It shows:

- Data from a housing estate path which is subject to deterioration.

Appendix Contents

[C1 Information used for the example](#)

329

[C1 Information used for the example](#)

This an examination of a shortcut which was installed on a new housing estate designed to fit the architectural feel of the estate. Natural materials were used to create a countryside image. The effect was a green area with existing trees in the

centre and a path at the side next to a private drive. The shortcut is used by people walking from the top of the estate to houses at the bottom and also young cyclists using the ground as a rally race stage on mountain bikes. The path's gravel surface provides an opportunity to gain speed and perform a skidding stop at the bottom of the hill. This action tends to break up the path surface.

A road runs at right angles to the path at the bottom of the hill. The road is separated from the path down the hill by a small paved area ending in a curb. Cars use the road as the main access to the lower part of the estate.

When the weather is bad rain cascades down the path washing some of it away leaving an uneven surface and exposed water meters in the path.

Images have been taken from the David Wilson Home site.

Images: David Wilson homes <https://www.dwh.co.uk/new-homes/city-of-derby/h723801-david-wilson-homes-@mickleover/>



Figure 40 Site layout. Bottom of hill is Trent Way (David Wilson Homes, 2020)

As can be seen from Figure 40, the path runs along the left-hand side of the public open space. The gradient runs from Harper Drive down to Trent Way.

Figure 41 shows an artist's impression of the path.



Figure 41 Sales vision of path (David Wilson Homes, 2020)

Appendix D - Baildon incident particulars

Appendix contains the details extracted from the publicly available Baildon RAIB investigation report (Rail Accident Investigation Branch, 2017), that has been produced of their analysis.

Appendix Contents

D1 Narrative of information from the RAIB report	333
D2 Diagrams	336

D1 Narrative of information from the RAIB report

The information below is summarised from the RAIB report (Rail Accident Investigation Branch, 2017) into the Baildon incident to provide a context for the analysis

During heavy rain during 7 June 2016 part of the structure supporting the railway line was washed away by flood water flowing down an embankment. The incident was reported by members of the public and the Fire and Rescue service to

controllers at Network Rail but no effective action was taken and several trains passed over an unsupported section of track. The report majors on the failings of Network Rail in dealing with the reports but does not identify any major concerns with the design of the location. Trains were stopped and staff inspected track near the location but not the correct location and reported that the flood water had receded with no damage. Trains were then allowed to operate again and further reports of the washout were received. The recommendations were as follows:

- measures to minimise the risk of further washouts at Baildon
- improving the emergency response to incidents on the track by providing Network Rail responders with accurate location information
- improving the effectiveness of communicating safety critical information between incident controllers, signallers and drivers

The concern expressed by the RAIB is that the incident could have easily resulted in a derailment and consequential injuries and fatalities.

List of failures identified from RAIB report is shown in Table 36.

Table 75 Extracted list of causal factors from RAIB report

Ref	Primary causal factor	Secondary causal factor
1	Ballast under one rail washed out	<ul style="list-style-type: none"> g. Drainage could not cope with quantity of flood water h. Flood water directed onto single sided embankment i. Previous flood repair did not withstand water flow
2	Reports of track damage not dealt with appropriately	<ul style="list-style-type: none"> i. Controllers did not listen carefully to emergency calls j. Controllers misdirected responders to a different location k. Responders not aware of the vulnerability of embankment to flooding

		I. A third train was allowed to traverse the washed-out track section when the line was blocked
--	--	---

There are in effect three events, first there is a washout and second trains traversed the washed-out section of line and finally a train traversed the washout after it should have been stopped. These are sequential and therefore like (Heinrich 1931) dominos, cited by Reason, Hollnagel and Paries (2006), the removal of anyone of them will stop the rest. Logically considering the risk of an accident it will only occur when the train operates over the washed-out section and therefore operation of further trains is not really of concern regarding the primary incident as the risk has already been present.

The last secondary cause (2d) in Table 36, does not refer to the primary incident that allowed the incident to occur in the first place and therefore has been discounted from the analysis.

Table 76 List of failure findings from RAIB report related to the washout event

Finding	Post or pre-event finding
Wrong section inspected / section missed	Post event
Track washed out for 4m	Event
Drainage could not cope	Pre-event
Previous washout had been repaired	Pre-event

D2 Diagrams

A drawing has been created by RAIB to allow a visualisation of the land at the site of the incident.

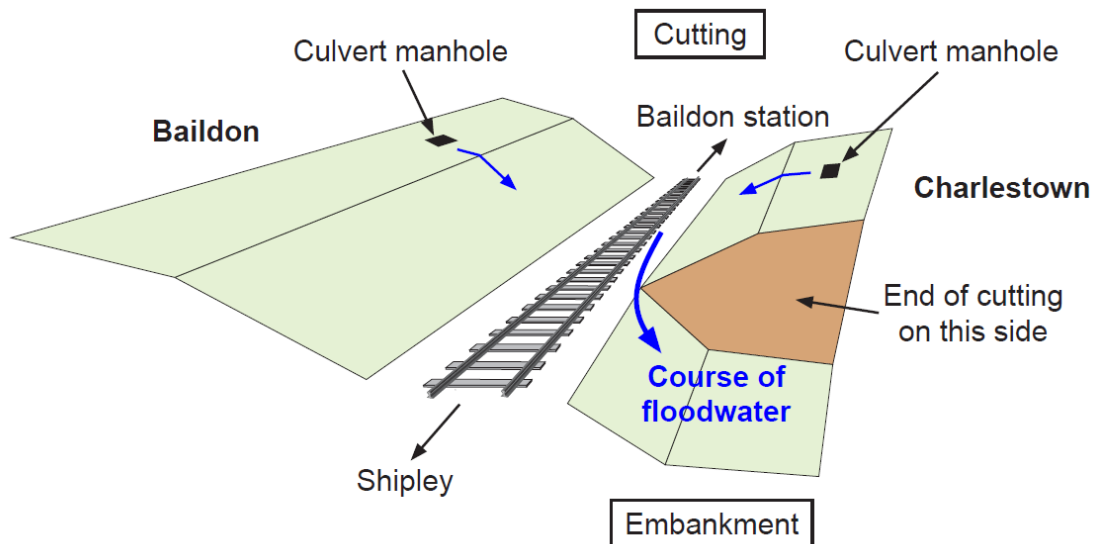


Figure 42 Embankment diagram and water flow from RAIB report

As can be seen from Figure 40, water flows out from the culvert inspection hatches down the embankment. This implies that the inspection manholes are acting as a pressure relief for the culvert.

Taken from the RAIB report, Figure 41 indicates the catchment area for the flood water that is designed to flow through the Barnsley Beck and culvert from the upper side of the railway to the downhill side. After the railway the Beck drains into the river Aire.

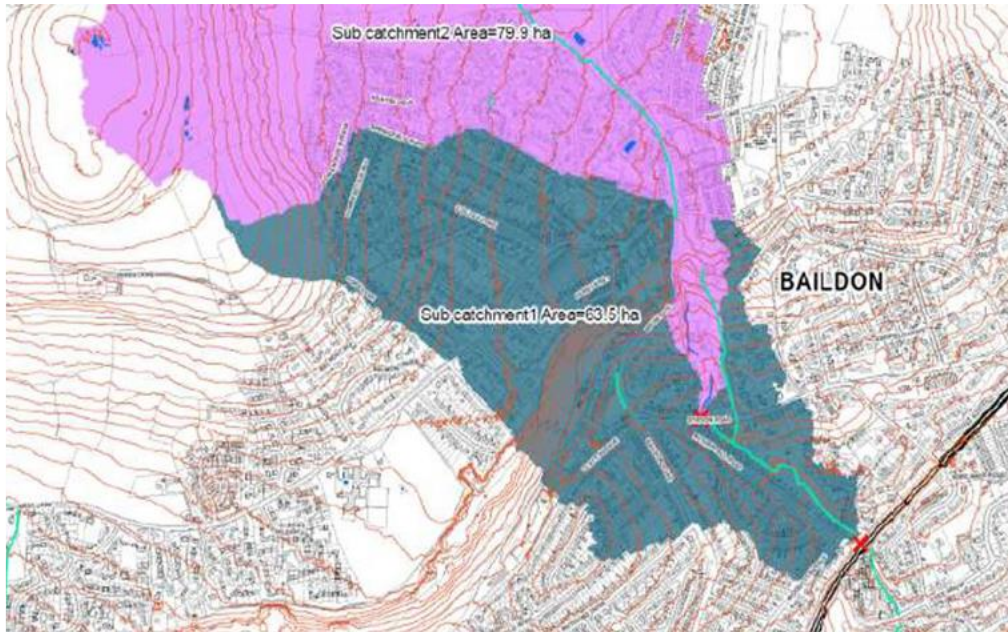


Figure 43 Water catchment area for RAIB report

A cross section diagram, Figure 44, was provided to show the position of the culvert, manholes and embankment at the site. It should be noted that the culvert as drawn is further up the line towards Baildon station than the site of the washout. Water flows from this point in the cutting to the point where one side of the embankment stops and this is where the washout occurs, as the water can then runaway downhill towards the river.

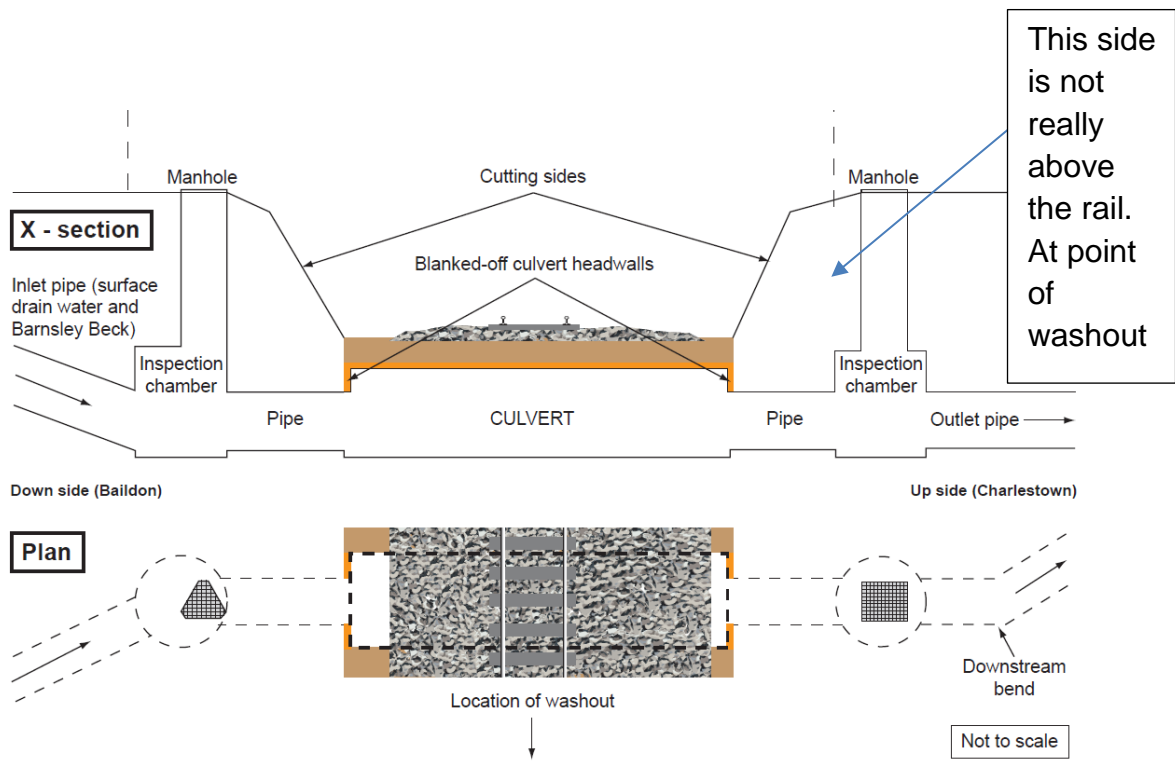


Figure 11: The culvert and its connections to the drainage system

Figure 44 Cross-section of culvert from RAIB report

D3 Facts extracted from the report

This section contains a set of facts extracted from the report to establish a single list of information for the subsequent analyses. This will mitigate against varying and increasing understanding of the report through multiple passes. As a result, it will help preserve the internal integrity of the analysis.

The type column is used in Chapter 7 for a type of cluster analysis. Py=Physical fact, Pr=Process fact.

Incident facts

Type	Ref	Fact
Py	1	A portion of the beck drainage runs under the railway in a culvert
Py	2	Water came out of the drainage manholes and ran down the sloped land to the railway and along the track until it reached a point where one side of the embankment stopped and the water ran over the side draining into the allotments on lower side of the raised track.
Pr	3	The duty Mobile Operations Manager could not go onto the railway because he was medically unfit
Pr	4	The Mobile Operations Manager initially went to the wrong location (bridge 2 not bridge 7).

Pr	5	The Emergency services contacted Network Rail control with a message from a member of the public that the track had been washed out. This was at 16:29 just before the first train passed the site of the incident. However, well before the other trains (17:45 and 17:59)
Py	6	A train passed over the washed-out track.
Pr	7	A further call from the Emergency services was interpreted by Network Rail control as flooding.
Pr	8	Inspections were arranged to look for flooding. The washed-out track was 250m south of the inspected area.
Pr	9	The line was reopened and two further trains passed over the wash out.
Pr	10	The third train driver saw wash out but could not stop and reported the wash out at a signal.
Pr	11	The separate controllers were involved in receiving calls from the emergency services. This involved message passing to controller 2.
Pr	12	The controller responsible for the area is controller 2
Py	13	The lower side of the beck runs toward the river Aire
Pr	14	The line was blocked by the signaller after the first train had passed because of moving flood water in accordance with the rule book.
Pr	15	The rule book rule for blocking the line is a mitigation against ballast being washed away.
Pr	16	During a call received from the emergency service controller 1 made an incorrect assumption of the location of the reported damage and thought it was being dealt with.
Pr	17	Controller 2 did not tell either the Track Technician or the Mobile Operations Manager the exact location of the reported damaged track only it was near bridge 7.
Pr	18	The Mobile Operations Manager reported no damage, but he then realised he was at the wrong location bridge 2.
Pr	19	The Track Technician inspected about 100m of track and reported water on the railway and cess but not movement of the ballast.
Pr	20	The Track Technician reported that it was safe to open the railway
Pr	21	A third call from the emergency services to the control reported that the rails were bent and the track was floating in air.
Pr	22	After the third call the controller instructed the signalling shift manager to block the line because of a landslip. The signaller immediately blocked the line.
Py	23	After the incident the Track Section Manager visited and established that 6 sleepers were unsupported.
Py	24	The rails are mounted on concrete sleepers.
Py	25	The sleepers were on top of ballast which is on clay soil.

Contextual facts

Type	Ref	Fact
Py	1	Water drains from the urban area on the high side of the railway to the lower side through a culvert structure which is 180m long. It was originally built for the purpose of allowing the railway to pass over the beck when the railway was constructed.
Py	2	The local council modified the feed into the culvert by connecting drainage pipes and building inspection hatches at each end. The pipes cut the capacity for flow through the culvert by one third.
Py	3	The beck was originally an open channel but has been built over and enclosed. Note this changes the channel into a pipe system.
Py	4	The section of track had been washed out two years earlier and repaired.
Pr	5	The drainage system was not investigated after the previous flood.
Pr	6	The network Rail previous incident report recommended a piped drainage system to capture any overflow water from the manholes and direct it to a soak away ditch. It was not implemented
Pr	7	Reconstruction of the embankment to withstand wash out after that previous incident was not implemented

Appendix E - Test case - Grayrigg CAM risk analysis

The Author has conducted a CAM risk assessment on the Grayrigg accident in this appendix. Grayrigg was a significant accident on the mainline GB railway during 2007, where a fatality occurred due to a derailment. The accident is referred to as Grayrigg, however the points (rail switches) concerned are at Lambrigg, hence the accident is occasionally referred to by industry workers as the 'Lambrigg incident' which leads to the impression by the public that they are two separate accidents. The accident has been recognised as significant not only because a RAIB report has been produced but also the accident has been used to benchmark other techniques as reported by Underwood and Waterson (2013b), which provides an opportunity to gauge the relative success of CAM against another reference.

This test case has been carried out using the publicly available information from RAIB accident report (Rail Accident Investigation Branch, 2011) as the source data for the analysis.

Appendix Contents

E1 Assessment of risk	342
E2 Method used	344
E3 Summary of the accident	346
E4 Analysis	346
E4.1 FMEA	349
E4.2 CAM Combinator	356
E4.3 Combined system cause consequence table	362
E4.4 Summarised risk matrix	365

E1 Assessment of risk

The Author has used a semi-qualitative method of assessing risk and risk acceptability for this test case. The reference for the method is based on EN50126 (CENELEC, 2017), shown in Table 77, as a calibrated likelihood-consequence table. The Author has calibrated the table to align with the guidance from the ORR (Office of Rail and Road, 2018).

Table 77 Risk matrix formulated from (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic	
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable	<1yr
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable	<2yrs
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable	<5yrs
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable	<10yrs
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	<20yrs
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	≥20yrs

The columns represent consequences and the rows are likelihood, risks are indicated by the product of consequence and likelihood in a cell. The green areas denote risks that are 'broadly acceptable', yellow are risks that are 'tolerable' if they are reduced to an ALARP level and red represent 'intolerable' risks.

E2 Method used

The analysis method used is as explained in Chapter 6, and documented in Appendix J (CAM user instructions) Section J2 and labelled as CAM-FN (Forward New/novel/modified analysis). The Author has decided for the purposes of this test case that the CAM-FN variant is more appropriate than the accident variants because the objective is to see if a CAM analysis produces a set of outputs rather than attempt to trace the causes from an incident.

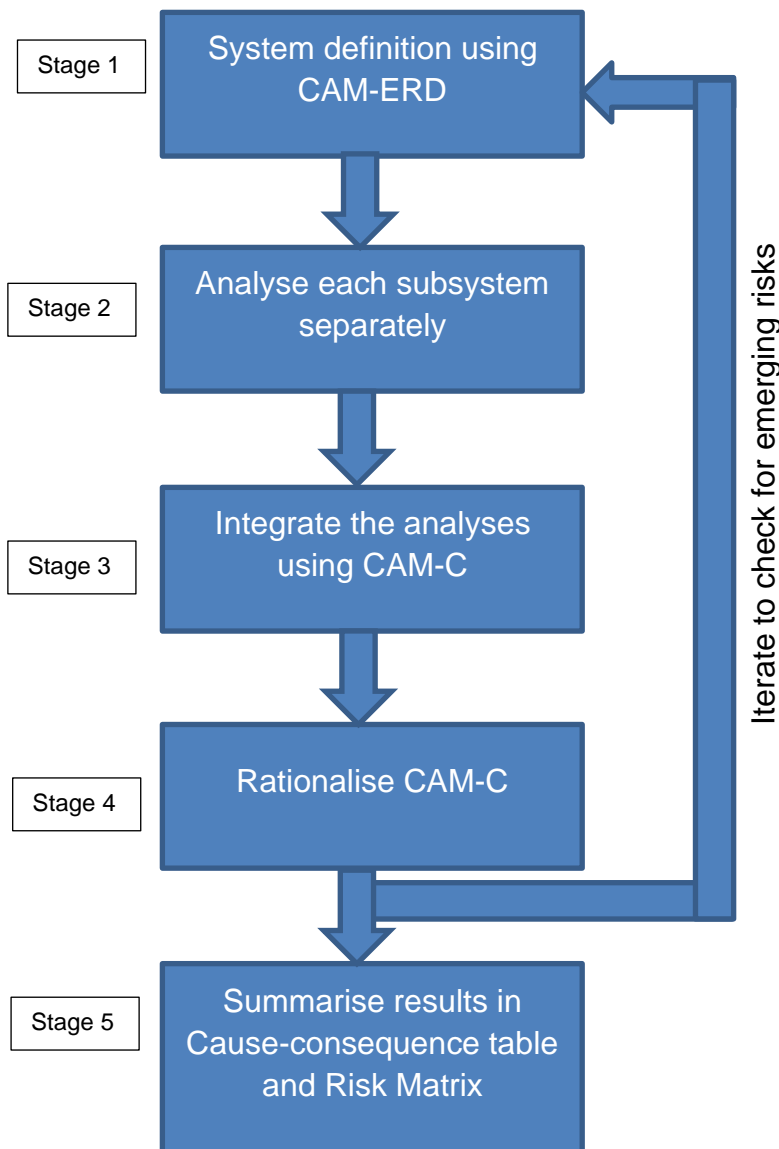


Figure 45 CAM_FN process reproduced from Appendix J

For this analysis FMEA has been selected as the method for the subsystem analysis because it was found to be the most popular from the industry analysis in Chapter 4.

The boxed 'Stage' labels in Figure 45 refer to stages in the CAM process which are explained in the user instructions in Appendix J. These labels are also used to indicate which part of the application of the process is being described in this appendix and feature as bold underlined headings.

E3 Summary of the accident

The train consisting of 9 cars and travelling at 95 mph was derailed at Lambrigg 2B facing points, which were an emergency crossover. Eight of the cars came to rest at the bottom of an embankment with five overturned. One person suffered a fatal injury and many others were injured.

Stretcher bar and out of tolerance adjustment failures left the switch rail free to move on the failed points causing the derailment by allowing the wheels to pass on the wrong side of the rails.

The report notes that the deterioration of the points took place over a period of time between the incident and at least eleven days before when an inspection was missed. This is based on an assumption that the inspection was scheduled on that day and that no significant deterioration would have occurred prior to that if the inspection periodicity set by the standard was adequate. Data from the New Measurement train indicates that the joints were missing from the second stretcher bar, indicating that there is a gradual deterioration of the integrity of the points.

E4 Analysis

Stage 1

The initial task is to create an CAM-ERD entity-relationship diagram of systems and subsystems. Table 78 has been created from the information in the RAIB report (Rail Accident Investigation Branch, 2011) as an aid to identify the various subsystems to insert into the CAM-ERD.

Table 78 Systems table

Main sub-system or system	Components/actors	Comments
Switch	<ul style="list-style-type: none">• Switch rails• Stock rail• Lock• Fixings & Bolts• Stretcher bars	The switch is a complex system with many parts some moving some fixed
Train	<ul style="list-style-type: none">• Wheelsets• Carriages	
People	<ul style="list-style-type: none">• Track Maintenance engineer (TME)• Trackworkers• Passengers• Driver• Area Maintenance Mgr	
Measurement train	<ul style="list-style-type: none">• Technicians• Measuring sensors• Reporting	This could be regarded as a process
Processes	<ul style="list-style-type: none">• Working hours• Inspection frequency• Maintenance tasks	

Figure 46 shows the CAM-ERD developed from Table 78. The circles represent subsystem clusters, rectangles are parts and the red triangle is the point of harm. Relationships are denoted by arrows; the labels represent risks and other activities that assist in understanding the system.

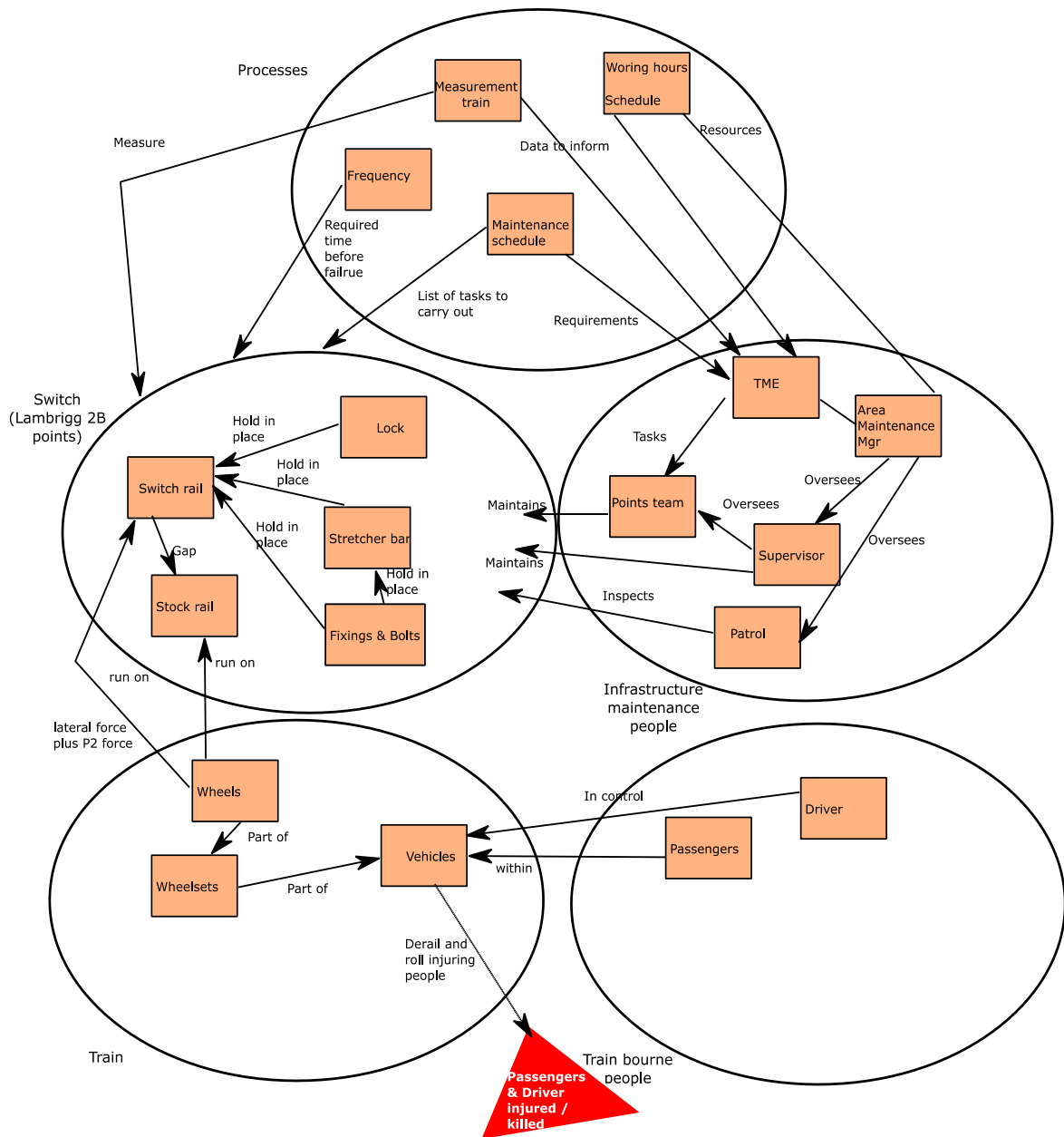


Figure 46 CAM-ERD Relationship diagram

As can be seen the harm comes from the vehicle derailing and rolling. Furthermore, there are many relationships that emanate from the maintenance process subsystem, which indicates that this may be driving the accident process.

E4.1 FMEA

Stage 2 – subsystem analysis

A desktop FMEA analysis has been conducted using EN60821 (CENELEC, 2006) and Anleitner (2010) and tailored to a safety application in a similar way to Mohr (2002). The approach has been to treat the systems as performing a function and then to document the failure of the function. A high detection number of 10 indicates that it will be easy to detect and prevent through the applied controls, conversely a low score indicates that the failure is difficult to detect and therefore may be latent. The classification is S for a significant function failure and C for a critical failure where there is a direct safety implication. Classification conversions, if necessary, from S to C are performed by adjusting the occurrence to reflect that not every failure will result in a safety event as articulated by Lepmets (2017). Also, consideration will be taken of the effect of detection and controls when setting the occurrence in the case of a safety classification. The RPN field is not considered appropriate for this particular application.

The scale for the severity and conversion of the frequency to a scale used in the risk matrix are given in Table 79 and Table 80 below in preference to the normal 10-point scale.

Table 79 Scaling table for occurrence formulated from (CENELEC, 2017)

Occurrence Category	Value	Definition
Frequent	6	Less than a year
Probable	5	Less than 2 years
Occasional	4	Less than 5 years
Rare	3	Less than 10 years
Improbable	2	Less than 20 years
Highly Improbable	1	Greater or equal to 20 years

Table 80 Scaling table for the severity formulated from (CENELEC, 2017)

Category	Value	Safety Definition	Equipment failure definition
Catastrophic	5	Multiple fatalities	Multiple systems loss
Critical	4	Fatality/multiple major injuries	Major loss of system
Major	3	Life changing injury	Severe systems damage
Marginal	2	Injury	Minor systems damage
Insignificant	1	No material harm	

The FMEA assessment for the switch has been undertaken as though maintenance does not take place. This is accounted for later with the input of the maintenance teams.

Table 81 FMEA for switch

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
101	Stretcher bar	Maintain gauge of switch rails	Failure during operation	Snaps	Loss of gauge	5	S	Large impact force from train	2yr	Maintenance schedule Designed to withstand forces	Weekly patrol, scheduled inspection and surveys	10		Could be due to fatigue The maintenance schedule is designed to identify failures before a safety impact. There is only a problem if the maintenance is not done. This reduces the safety incidence to 10 years. However, the whole analysis is centred on applied maintenance. Hence failure figures are left unamended

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
102	Stretcher bar	Maintain gauge of switch rails	Failure during operation	Loose	Loss of gauge	5	S	Vibration from trains	6m	Maintenance schedule	Weekly patrol, scheduled inspection and surveys	10		The stretcher bar has a number of fixings and a single fixing cannot cause the bar to be loose. The points have a number of stretcher bars. Therefore, the failure of a single bar will not cause loss of gauge. The maintenance schedule is designed to identify failures before a safety impact. Overall, the incidence is reduced to 20 yrs. However, the whole analysis is centred on applied maintenance. Hence failure figures are left unamended
103	Joints	Hold parts together	Failure during operation	Parts separate	Derailment	5	S	Vibration or clamping force exceedance	1yr	Maintenance schedule	Weekly patrol, scheduled inspection and retorque	10		The maintenance schedule is designed to identify failures before a safety impact. The failure of a single joint will not cause a derailment because of the design. From a safety impact perspective, the incidence has been reduced to 5yrs. However, the whole analysis is centred on applied maintenance. Hence failure figures are left unamended
104	Stock rail	Provide fixed path for wheel	Failure during operation	Moves	Derailment	5	C	Fixings undone	2yrs	Maintenance schedule	Weekly patrol, scheduled inspection	7		Could be missed due to volume The maintenance schedule is designed to identify failures before a safety impact. There is only a problem if the maintenance is not done. There are multiple fixings on the stock rail that would have to be undone for a safety incident. However, the whole analysis is centred on applied maintenance. Hence failure figures are left unamended

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
105	Switch rail	Provide movable path for wheel	Failure during operation	Moves undertrain	Derailment	5	C	Fixings undone	2yrs	Maintenance schedule	Weekly patrol, scheduled inspection	7		Could be missed due to volume The maintenance schedule is designed to identify failures before a safety impact. There is only a problem if the maintenance is not done. The switch rail performance is tied to the stretcher bar and fixings. However, the whole analysis is centred on applied maintenance. Hence failure figures are left unamended
106	Switch rail	Provide minimal gap at the toe with stock rail	Failure during operation	Gap too big	Derailment	5	C	Gap too big wheel misses switch rail	1yrs	Maintenance schedule	Weekly patrol, scheduled Inspection and measurement	10		The maintenance schedule is designed to identify failures before a safety impact. However, the whole analysis is centred on applied maintenance. Hence failure figures are left unamended

Table 82 FMEA for train

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
201	Wheel	Follow the path of the rail	Failure during operation	Climb rail	Derailment	5	C	Loss of rail integrity	20yr	Maintenance schedule of rails	Inspection and surveys	10		The system is designed to avoid a rail climb
202	Wheel	Follow the path of the rail	Failure during operation	Climb rail	Derailment	5	C	Deformed wheel profile	20yr	Maintenance schedule	Inspection and surveys	10		

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
203	Wheelset	Constrain wheelsets	Failure during operation	Frame or suspension components break	Derailment	5	C	Fatigue or large impact	5yrs	Maintenance schedule	Inspection and surveys	10		
204	Vehicle	Crush resistance	Failure during crash	Structure buckles	Reduced survival space	5	C	Impact or rollover	10yrs	Wheelsets and rail integrity, vehicle structural integrity	Inspection and surveys	10		History has shown that the vehicles to an extent tend to deform when they roll

Table 83 FMEA for train people

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
301	Driver	Control train speed	Failure during operation	Overspeed	Derailment	5	C	Ignore conditions	2yr	Training and supervision	Driving records	10		Speeding does happen but trains stay on the track more often than not

Table 84 FMEA infrastructure maintenance people

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
401	Area Mgr	Set work schedule and make resource available	Failure during operation	Schedule too much work	Maintenance work not done	3	S	Over optimism	1yr	Audits	Records	5		There are safeguards built into the systems that mitigate missed maintenance. Safety impact is spread across an organisation and most likely to show up in a smaller incident
402	Points team	Carry out maintenance tasks	Failure during operation	Task not carried out	Defective equipment	3	C	Slip or violation or not enough time	1yr	Safety factors in design. Audits and supervision	Records	3		Initially the missed tasks may result in a function not working correctly but compensated for by other features of the design. As more is missed overtime the potential number failures are likely to become critical where design compensation fails.
403	Supervisor	Carry out and supervise key maintenance tasks	Failure during operation	Failure to make sure task is carried out	Defective equipment	3	C	Slip or violation or not enough time	1yr	Safety factors in design. Audits and supervision	Records	3		
404	Patrol	Inspect track	Failure during operation	Miss track and switch faults	Defective equipment	4	C	Inspection cursory and not as specified	3m 2yrs	Safety factors in design and revisits	Records	5		The evidence shows that the track patrol did take place with 8 people on a weekly basis. The frequency is likely act to show missed elements. Consequently, the occurrence has been adjusted to take account of this. Although there is a limit as to what can be observed.

Table 85 FMEA processes

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
501	Working hours	Limit the number of hours and inspect in daylight	Failure during operation	Work does not match available hours	Maintenance work not done	3	C	Over optimism	4yr 5yrs	Audits	Records	5		Overall, some of the work will lead to reliability issues rather than safety. Standards are designed to allow for a number of missed maintenance points. The safety critical task subset of work is essential and captured below and frequency adjusted to 5yrs. Safety impact is spread across an organisation and most likely to show up in a smaller incident
502	Frequency of tasks	Carry out tasks within a set period	Failure during operation	Work not listed before potential failure	Maintenance work not done	3	C	Over optimism	4yr 5yrs	Audits Engineering assessment	Records	5		It is essential that maintenance task frequency is greater than the time to failure so even if a task is missed there is another chance to carry it out before a critical point is reached. As a result, the safety critical element has been adjusted to 5yrs Safety impact is spread across an organisation and most likely to show up in a smaller incident
503	Maintenance schedule	List tasks to be carried out on a visit	Failure during operation	Work not completed	Maintenance work not done	3	C	Over optimism	4yr 5yrs	Audits Engineering assessment	Records	5		It is essential that maintenance task frequency is greater than the time to failure so even if a task is missed there is another chance to carry it out before a critical point is reached. As a result, the safety critical element has been adjusted to 5yrs Safety impact is spread across an organisation and most likely to show up in a smaller incident

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
504	Measurement train	Automatically inspect infrastructure	Failure during operation	Data not reviewed	Defective equipment	4	C	Too much data	3m	Engineering tools and audits	Records	3		There is a reliance on automatic collection of data which is of no use if no one looks at it.
505	Safety critical maintenance plan	Plan for safety critical tasks to fit within working hours	Failure during operation	Tasks not completed	Defective equipment	4	C	Too much work planned for resources	1yr	Audits, prioritisation, Standards	Records	4		Safety impact is spread across an organisation and most likely to show up in a smaller incident

E4.2 CAM Combinator

Stage 3

The CAM-C is laid out below. The convention adopted is input columns and outputs are rows. This can be interpreted as the columns acting as causes for the hazard indicated in the rows. Using the CAM Combinator, a chain of events can be traced through the system. The individual entries can be traced back to the FMEAs through the 'Ref' entry. Using the CAM-C, a chain of events can be traced through the system which is described in Appendix J Section J2. The individual entries can be traced back to the FMEAs through the 'Ref' entry e.g. 101. The resulting matrix is much larger than the previous applications, which reflects a more complex system. However, it is clear from the CAM-C that the main interaction is between the processes (in the 500 range) and the point components, because of the cluster of links in the top righthand corner of Table 86.

Table 86 Grayrigg CAM Combinator

		Ref		101	102	103	104	105	106	201	202	203	204	301	401	402	403	404	501	502	503	504	505	
Switch	Stretcher bar																							
		101	Snaps			3			2															
		102	Loose			3													2	2	2	2	3	
	Joints																							
		103	Parts separate														3	3	2	2	2	2	3	3
	Stock rail																	2						
		104	Moves																					
	Switch rail																							
		105	Moves undertrain	2	2															2	2	2		3
	106	Gap too big														2	3		2	2	2	3	3	
Train system	Wheel																							
		201	Climb rail					3	3															
		202	Climb rail																					
	Wheel set																							
		203	Frame or suspension components break							2														
	Vehicle																							
	204	Structure buckles							2															
Train people	Driver																							
		301	Overspeed																					
People system	Area Mgr																							
		401	Schedule too much work																	3				
	Points team																							
		402	Task not carried out													2								
	Supervisor																							

Stage 4

The system where harm takes place is the train. As per the CAM-ERD the train is taken as a whole in this analysis and consists of those items in the 200 series. The Author has chosen to collect all the risks associated with the train and treat them as a single system level entity because this is the point of harm. The CAM-C has shown that there is a concentration of links between the processes and the points which is to be expected. The extent of further rationalisation is to replace the system level train risks with the root causal risks using the trace and rationalisation process described in Appendix J. In addition, there are no terminator links identified and therefore the underlying subsystem behaviour is not masked from the overall system.

As can be seen the two key items are the infrastructure maintenance people and the processes. The CAM-C also highlights that the switch system is critically dependent on the joints which is the primary cause of the incident. However, its integrity is dependent on the two identified subsystems. It is also clear that other subsystems were not implicated in this incident.

Iteration

The integration of the subsystems into a whole system view has been reductionist and new hazards have not emerged therefore a review of stages 1 to 4 is not necessary in this case.

Stage 5

Table 87 has been constructed by collecting together those items that were identified as either a carrier, resistor or amplifier. In addition, a column has been appended to the right to indicate the level increase or decrease when the cause is referred to the system level. A value of 1 is a one-level increase in the likelihood, when the overall value is calculated, other values will create a different number of category increases or decreases. Those that were identified as an amplifier have had the frequency adjusted to reflect the increased risk in this configuration of the total system. In this case a doubling of the frequency was judged appropriate. Frequency was chosen because the consequence increase cannot be justified in this particular case. These adjustments are shown in red in Table 87.

Table 87 System level FMEA table

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Increase at sys level
101	Stretcher bar	Maintain gauge of switch rails	Failure during operation	Snaps	Loss of gauge	10	C	Large impact force from train	2yr 1yr	Maintenance schedule Designed to withstand forces	Weekly patrol, scheduled inspection and surveys	10		1
102	Stretcher bar	Maintain gauge of switch rails	Failure during operation	Loose	Loss of gauge	10	C	Vibration from trains	6m 3m	Maintenance schedule	Weekly patrol, scheduled inspection and surveys	10		1
103	Joints	Hold parts together	Failure during operation	Parts separate	Derailment	10	C	Vibration or clamping force exceedance	4yr 3m	Maintenance schedule	Weekly patrol, scheduled inspection and retorque	10		2
105	Switch rail	Provide movable path for wheel	Failure during operation	Moves undertrain	Derailment	10	C	Fixings undone	2yr 1yr	Maintenance schedule	Weekly patrol, scheduled inspection	7		1
106	Switch rail	Provide minimal gap at the toe with stock rail	Failure during operation	Gap too big	Derailment	10	C	Gap too big wheel misses switch rail	4yr 6m	Maintenance schedule	Weekly patrol, scheduled inspection and measurement	10		1
401	Area Mgr	Set work schedule and make resource available	Failure during operation	Schedule too much work	Maintenance work not done	7	C	Over optimism	4yr 1m	Audits	Records	5		3
402	Points team	Carry out maintenance tasks	Failure during operation	Task not carried out	Defective equipment	7	C	Slip or violation or not enough time	4m 1m	Safety factors in design. Audits and supervision	Records	3		3

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Increase at sys level
403	Supervisor	Carry out and supervise key maintenance tasks	Failure during operation	Failure to make sure task is carried out	Defective equipment	7	C	Slip or violation or not enough time	4m 1m	Safety factors in design. Audits and supervision	Records	3		3
404	Patrol	Inspect track	Failure during operation	Miss track and switch faults	Defective equipment	8	C	Inspection not detailed	2yr 6m	Safety factors in design and revisits	Records	5		2
501	Working hours	Limit the number of hours and inspect in daylight	Failure during operation	Work does not match available hours	Maintenance work not done	7	C	Over optimism	5yr 1yr	Audits	Records	5		2
502	Frequency of tasks	Carry out tasks within a set period	Failure during operation	Work not listed before potential failure	Maintenance work not done	7	C	Over optimism	5yr 1yr	Audits Engineering assessment	Records	5		2
503	Maintenance schedule	List tasks to be carried out on a visit	Failure during operation	Work not completed	Maintenance work not done	7	C	Over optimism	5yr 1yr	Audits Engineering assessment	Records	5		2
504	Measurement train	Automatically inspect infrastructure	Failure during operation	Data not reviewed	Defective equipment	8	C	Too much data	3m 2 wk	Engineering tools and audits	Records	3		3
505	Safety critical maintenance plan	Plan for safety critical tasks to fit within working hours	Failure during operation	Tasks not completed	Defective equipment	8	C	Too much work planned for resources	4yr 1m	Audits, prioritisation, Standards	Records	4		3

E4.3 Combined system cause consequence table

The cause-consequence table is drawn together from the system level FMEA and developed into a risk expression through the application of Table 77.

As highlighted by Lepmets (2017), the common currency between a FMEA and hazard analysis is the expression of the cause. The consequence and likelihood are influenced by the FMEA and where the failure is denoted as a safety failure the consequence will be the same.

If the process controls were in place the occurrences would have been significantly reduced and many of the risks would have been tolerable. However, the evidence points to the fact that the controls were not followed. Therefore, the profile tends to follow the raw component defect rates.

Table 88 Cause-consequence table

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Control	Evaluation type	Likelihood	Consequence	Risk
101	Stretcher bar snapped	Loss of gauge	Large impact force from train	Stretcher bar does not constrain the switch rails and there is a potential for a derailment	Rails move from set position	Derailment	Maintenance schedule Designed to withstand forces	Risk Estimation	Probable	Catastrophic	Intolerable
102	Stretcher bar loose	Loss of gauge	Vibration from trains	Stretcher bar subject to repeated forces beyond the clamping force causing fixings to become loose	Rails move from set position	Derailment	Maintenance schedule	Risk Estimation	Frequent	Catastrophic	Intolerable
103	Fixings part	Switch falls apart	Vibration or clamping force exceedance	Trains cause the fixings to come loose and eventually fall apart. At this point the switch has fallen apart	Parts move from the design position and train falls off the rails	Derailment	Maintenance schedule	Risk Estimation	Frequent	Catastrophic	Intolerable
105	Switch rail moves	Rail moves under train	Fixings undone	Rail moves under the force of the train because the fixings do not	Parts move from the design position and train falls off the rails	Derailment	Maintenance schedule	Risk Estimation	Probable	Catastrophic	Intolerable

				hold the rail in place							
106	Gap too big	Switch rail gap too big	Gap is not set correctly	The gap is too big and causes the train wheel to pass on the wrong side of the switch rail	Train loses gauge and falls off the rails	Derailment	Maintenance schedule	Risk Estimation	Frequent	Catastrophic	Intolerable
401	Work schedule not viable	Maintenance work not completed	Work schedule does not match available resources	There are not enough resources to carry out the work	Defective equipment left uncorrected	Derailment	Audits	Risk Estimation	Frequent	Critical	Intolerable
402	Maintenance tasks missed	Maintenance tasks not completed	Points team miss maintenance tasks	The points team do not carry out all the maintenance tasks on the points	Defective equipment left uncorrected	Derailment	Safety factors in design. Audits and supervision	Risk Estimation	Frequent	Catastrophic	Intolerable
403	Supervision failure	Maintenance tasks not completed	Supervisor fails to make sure work is complete	The points team do not carry out all the maintenance tasks on the points	Defective equipment left uncorrected	Derailment	Safety factors in design. Audits and supervision	Risk Estimation	Frequent	Catastrophic	Intolerable
404	Patrol miss defects	Defects not identified	Patrol inspections not detailed	The patrol inspects a large volume of equipment and only scans equipment	Defective equipment left uncorrected	Derailment	Safety factors in design and revisits	Risk Estimation	Frequent	Catastrophic	Intolerable
501	Not enough working hours	Maintenance work not completed	Resources available do not match workload	The restrictions on working hours mean there is not enough time to carry out the required work	Defective equipment left uncorrected	Derailment	Audits	Risk Estimation	Probable	Critical	Intolerable
502	Frequency not enough	Missed tasks become critical	The frequency too low	The set frequency of maintenance tasks does not allow for a miss before it	Defective equipment left uncorrected	Derailment	Audits Engineering assessment	Risk Estimation	Probable	Critical	Intolerable

				becomes likely to fail							
503	Maintenance schedule not viable	Maintenance tasks not completed	Too many tasks for time available	There are too many tasks in a single visit to be completed	Defective equipment left uncorrected	Derailment	Audits Engineering assessment	Risk Estimation	Probable	Critical	Intolerable
504	Data overload	Defects not identified	Too much data	There is too much data to review	Defective equipment left uncorrected	Derailment	Engineering tools and audits	Risk Estimation	Frequent	Critical	Intolerable
505	Critical tasks not properly planned	Missed critical tasks	Too much work planned for resources	The resources do not match the planned critical work	Defective critical equipment left uncorrected	Derailment	Audits, prioritisation, Standards (require closure if not done)	Risk Estimation	Frequent	Critical	Intolerable

Hazards 401, 501, 502, 503, 504 and 505 have been judged to have less severe consequences because they apply throughout the organisation and would tend to show up as a trend where there are less severe consequences. As a result, there is more opportunity to correct these elements. Items 402 and 403 are to do with execution on the points in question where there were catastrophic consequences.

E4.4 Summarised risk matrix

A risk matrix has been drawn up from the cause-consequence table to indicate the extent of the risks.

Table 89 Grayrigg risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent				401, 504, 505	102, 103, 106, 402, 403, 404
Probable				501, 502, 503	101, 105,
Occasional					
Rare					
Improbable					
Highly Improbable					

In the Author's experience a matrix with the level of risks shown is an indication of a process that is out of control, which in the event it was.

Appendix F - Test case - Hong Kong Metro incident CAM analysis

The objective of this illustrative CAM test case application is to identify the conditions to permit an acceptably safe resumption of testing and summarise the critical risk causes through a CAM analysis.

A report has been produced by the Hong Kong authorities (Electrical and Mechanical Services Department, 2019); currently this is the only source of information apart from news reports which appear to be drawn from the same source. Some general information is available from the Thales zone controller system from a presentation given to the Institution of Signalling Engineers (Thales Group, 2015). Therefore, the information is limited which has constrained the analysis.

The accident report referenced the signalling standard EN50129 (CENELEC, 2003) and a metro standard IEEE1474.4 (IEEE, 2011), which specifically deals with testing of CBTC systems. EN50129 is used to point out that a safety case is required, while IEEE1474.4 is used to highlight the need for operational testing.

Appendix Contents

F1 Summary of Incident	
F2 Assessment of risk	367
F3 Study	368
F3.1 Assumptions	370
F3.2 Process description	370
F3.3 Method steps	370
F4 Analysis	371
	373

F1 Summary of Incident

The incident took place during testing of a new signalling system on the MTR Tsuen Wan Line. The system is an automatic metro CBTC system which has been designed for high efficiency. Extra features were contracted to provide resilience when a failure occurred and avoid down time, effectively masking failures from the public. This resulted in a novel design using three zone controllers, whereas all previous installations of the system around the world used two configured as a 'master' and 'hot standby'. In this case, the further controller was designed to remain in 'warm standby' to take over when the other two fail. The warm standby holds all the necessary static data but is missing some of the dynamic data, presumably designed to avoid the scenario where the dynamic data creates a

'lock-up' state in the zone controllers. The tests being conducted were to confirm that the warm standby would operate as planned. Two trains collided on a cross-over, because the zone controller did not register that the crossover was already occupied before routing a second train onto the cross-over.

F2 Assessment of risk

The Author has used a semi-qualitative method of assessing risk and the acceptability of risk based on EN50126 (CENELEC, 2017), shown in Table 90, as a calibrated likelihood-consequence table. The Author has calibrated the table in alignment with guidance from the ORR (Office of Rail and Road, 2018).

Table 90 Risk matrix formulated from (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic	
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable	<1yr
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable	<2yrs
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable	<5yrs
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable	<10yrs
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	<20yrs
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	≥20yrs

The columns represent consequences and the rows are likelihood. Risks are a product of the consequence and likelihood which equates to a cell on the matrix. The green areas denote risks that are 'broadly acceptable', yellow are risks that are 'tolerable' if they are reduced to an ALARP level and red represent 'intolerable' risks.

F3 Study

The depth of the analysis is limited by access to information and the time available.

The approach is to use CAM in a reverse mode and build the system, hazards and causes from the accident. An overview CAM-ERD diagram is shown in Figure 48.

F3.1 Assumptions

- a) The signalling system has, in previous forms been shown to be reliable in many other signalling projects. Therefore, the signalling functionality of the zone controller is assumed to have been proven through field service.
- b) The mechanical infrastructure is fundamentally safe for operation. This assumption is supported by the continued operation of the railway under the old signalling system.
- c) Engineering processes have been applied to the zone controller design and production, to some extent following the salient standards. Clearly, from the report (Electrical and Mechanical Services Department, 2019) there is some doubt with regard to the rigour of this process.

F3.2 Process description

The approach is to undertake the analysis by applying CAM in reverse mode, the CAM-RA variant, where the analysis works back through the system in an iterative manner, passing through a number of cycles, where the focus of each cycle is guided by the previous one. The cycle is indicated in a column in the tables. A

specific rationalisation stage is not applicable in this context as the complexity of next stage will be determined by the previous stage.

A simple cause effect table is constructed below as a first stage in the analysis. Normally, these tables are supported through analysis documentation and the tables include mitigations, and barriers which are omitted from all bar the final stage. This is justified, because the outcome is a demonstration of applicability rather than a full-blown investigation. The likelihood, consequence and risk entries that would be expected from such a system have been scored through and a more appropriate rating inserted in the light of events.

F3.3 Method steps

The variant of the CAM process used for this analysis is CAM_RA (reverse accident). It is shown in Figure 47 and the user instructions that have been followed for the analysis are contained in Appendix J.

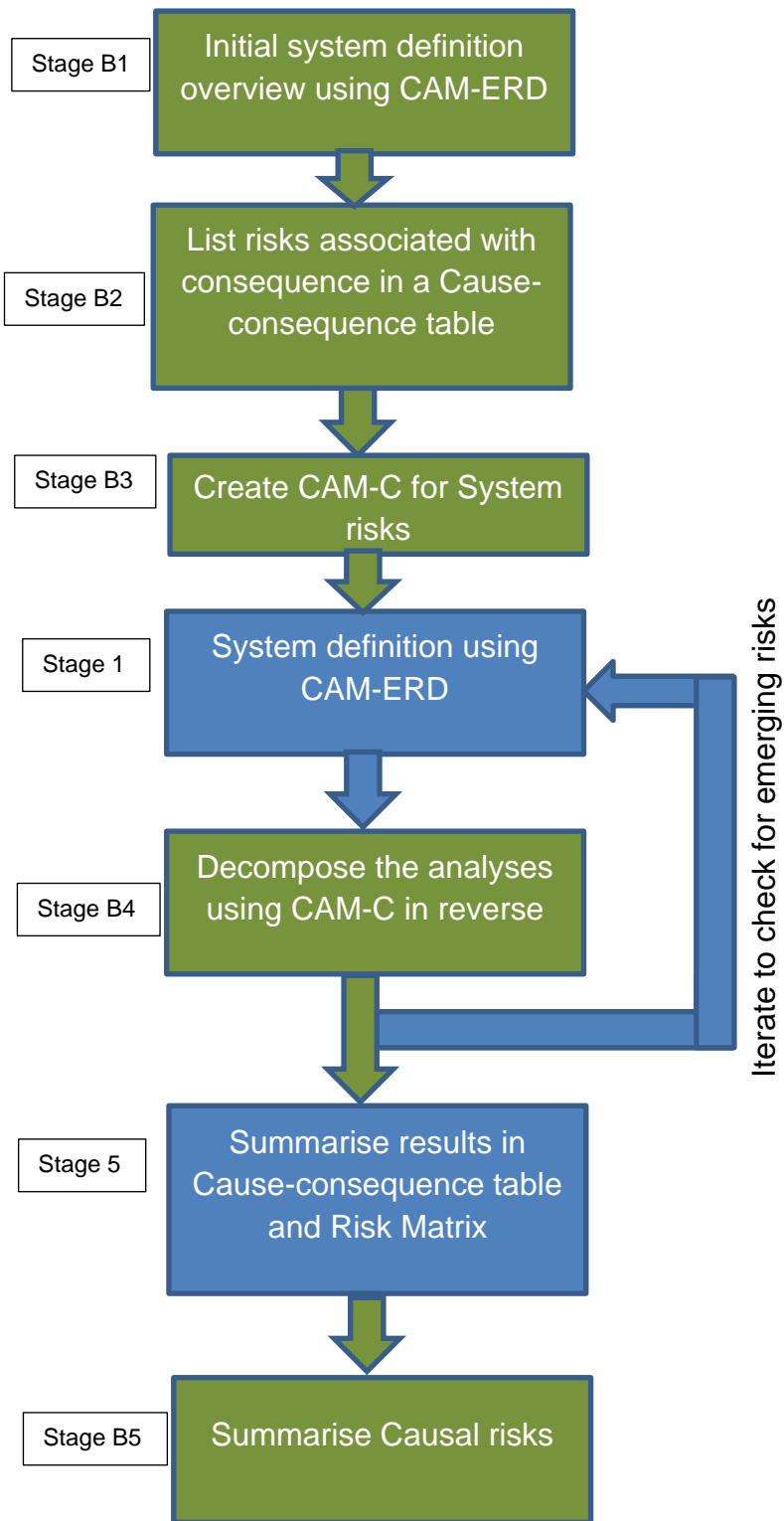


Figure 47 CAM_RA process reproduced from Appendix J

In addition, the output has been used to consider appropriate mitigations to reduce the risks, as per the test case objective to allow testing to restart safely.

The boxed 'Stage' labels in Figure 47 indicate the process stage that is explained in Appendix J. These labels are used in this analysis as bold underlined headers to indicate to which process stage the test is referring.

The red annotations in the analysis cause-consequence tables are the adjustments made as a result of the analysis

F4 Analysis

Stage B1

The initial CAM-ERD has been created from the information contained in the accident report (Electrical and Mechanical Services Department, 2019). The diagram has been constructed using the process described in Appendix J. Subsystems are denoted by circles and parts by rectangles and a point of harm by a red triangle. The relationships are denoted by arrows which are normally labelled with risks although other labels can be applied to assist with the understanding of the system to be examined.

In this case there are no subsystem circles due to the nature of the information provided. Instead, the parts have been colour coded with the 'level' of the subsystem. Yellow denotes the system level components (possibly major subsystems), brown are key parts that are linked to the system level components. The beige colour are lower level parts.

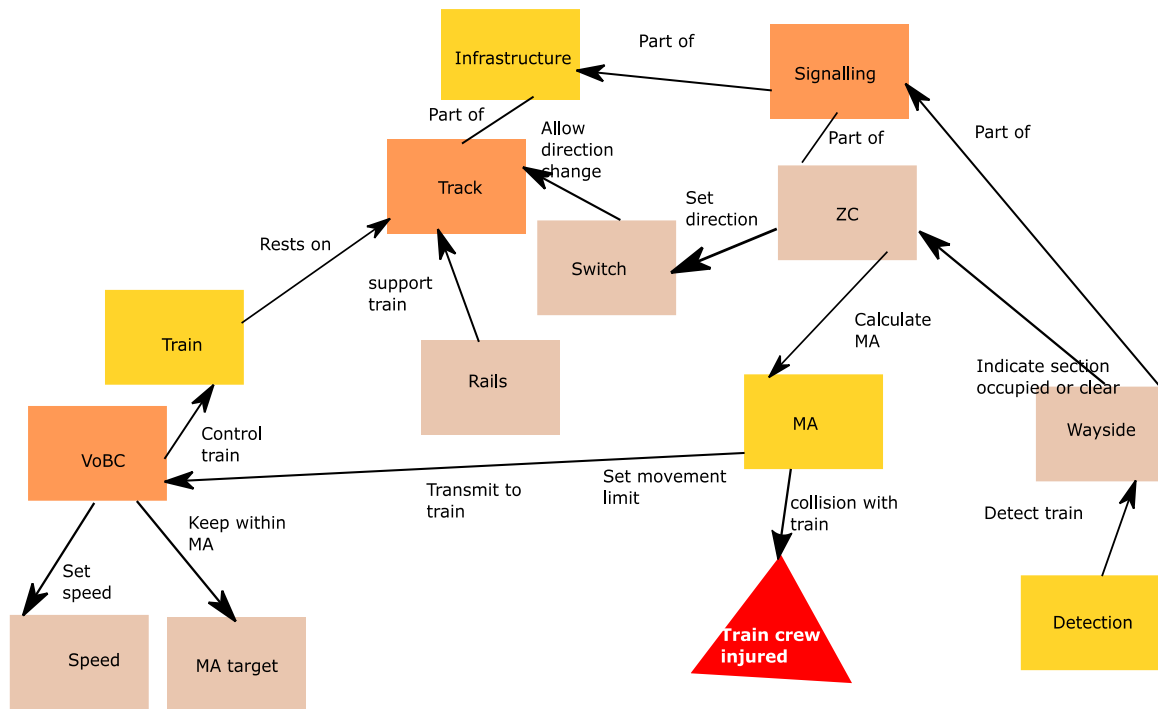


Figure 48 CAM-ERD overview relationship diagram

As can be seen from Figure 48, the zone controller is essentially at the heart of the system, receiving information about track occupancy, setting routes through the switch control and issuing movement authorities (MA) to trains. If the MA is wrong there is a high risk of a crash as pointed out in Electrical and Mechanical Services Department (2019) if the distance to an obstruction is incorrect.

Stage B2

The Author has populated the risk columns in Table 91 by using the descriptive accident information to judge the levels of risk and looking those values up from the reference risk values in Table 90.

An initial cause-effect table is constructed from consideration of the accident and the elements at the system level shown in initial CAM-ERD, Figure 48. This has

resulted in Table 91; which is a system level cause-consequence table. Notes have been attached in the last column as an aide to understanding the Author's rationale for the hazards listed.

Table 91 System level cause-consequence table

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
101	Trains off track	Track fails	The track formation fails and train leaves track and continues on ballast	Train collision	<ul style="list-style-type: none"> Track design Train speed Inspection 	Highly Improbable	Major	Negligible	<ul style="list-style-type: none"> It is clear that this did not happen as the track was intact
102	Switch setting wrong	Switch commanded to wrong position	Switch commanded to set a conflicting route	Train collision	<ul style="list-style-type: none"> Zone controller Through checks on commissioning 	Improbable	Catastrophic	Tolerable	
103	Train speeding	VOBC malfunction	Train is unable to maintain the speed profile due to a VOBC fault resulting is an overspeed and cannot stop	Train collision	<ul style="list-style-type: none"> A safety margin incorporated into infrastructure VOBC is a high integrity fail safe system 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> It is clear that this did not happen because it was shown the track was occupied within the MA

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
104	Train speeding leaves track	VOBC malfunction	Train is unable to maintain the speed profile due to a VOBC fault resulting in an overspeed and comes off the track	Train collision	<ul style="list-style-type: none"> • VOBC is a high integrity fail safe system 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • It is clear that this did not happen as the track was intact
105	Train outside MA	VOBC malfunction	Train is operating beyond the MA without the VOBC stopping the train	Train collision	<ul style="list-style-type: none"> • VOBC is a high integrity fail safe system • Zone controller should only grant routes to other trains when path is free 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • The zone controller is key to keeping separation even if the VOBC malfunctions through the control of other trains

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
106	Faulty MA issued	Zone controller malfunction	The zone controller issues an MA which is not valid and is in conflict with another train	Train collision	<ul style="list-style-type: none"> Zone controller is a high integrity unit and is a 2oo2 	Improbable Probable	Catastrophic	Tolerable Intolerable	<ul style="list-style-type: none"> The MA should not have been issued to train when crossover occupied
107	Zone controller faulty start up	Zone controller malfunction	The zone controller does not initialise and does not operate as per specification as a result fails to keep train separated	Train collision	<ul style="list-style-type: none"> Zone controller is a high integrity unit Zone controller is designed to comply with EN50128, IEEE1474 	Improbable probable	Catastrophic	Tolerable Intolerable	<ul style="list-style-type: none"> Evidence from the report shows that the system did not start up correctly
108	No train detected	The wayside detector is faulty	The detector fails to report an occupied track	Train collision	<ul style="list-style-type: none"> There are multiple detectors in wayside equipment 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> This did not happen

Stage B3

It is clear that the cause consequence table, Table 91, will lead to an extensive analysis of the system, which will require a huge effort, with little return. When applying CAM in reverse mode, rather than create a complete composite CAM-C, a CAM-C is created at each stage of the analysis to indicate which entries in the cause-consequence tables are supported by evidence. A CAM-C, as set out in Table 92, is used to focus the investigation on the key items from the overall systems analysis. This CAM-C is slightly different to the others because the columns are populated with consequences. This creates the mapping back to the system level hazards to initiate the iterative CAM-C process.

Table 92 CAM-C system level hazards – consequences

			Consequence property			
			Evidence	train out of control	MA incorrect	lineside error
Hazards	101	Trains off track	No			Yes
	102	Switch setting wrong	No			Yes
	103	Train speeding	No	Yes		
	104	Train speeding leaves track	No	Yes		
	105	Train outside MA	No	Yes		
	106	Faulty MA issued	Yes		Yes	
	107	Zone controller faulty start up	Yes		Yes	
	108	No train detected	No			Yes

As can be seen there are only two system level hazards that are relevant to the current investigation (106, 107), because these are the only two that are supported by evidence. The CAM-C indicates that the subsystem of interest is the zone controller.

Stage 1

The CAM-ERD is redrawn to reflect the new focus on the zone controller which was indicated in Stage B3 as the item to concentrate on.

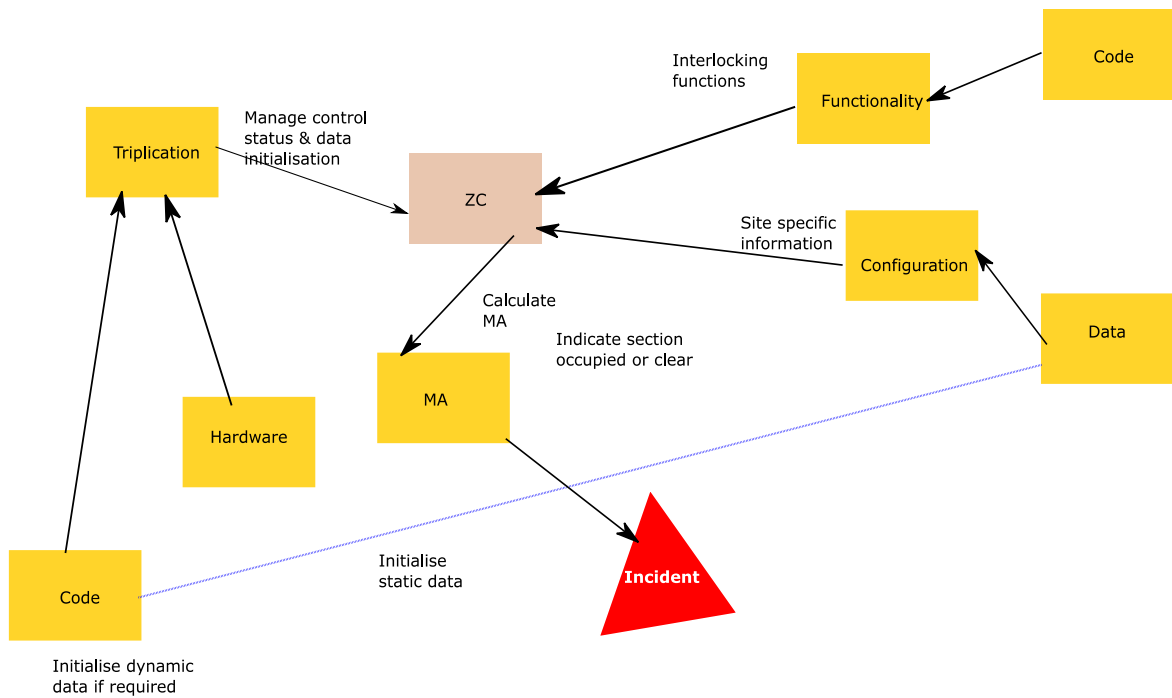


Figure 49 Developed CAM-ERD

Figure 49, shows that at the next level of decomposition the zone controller is a complicated subsystem with many parts. The key part of 'MA' is still retained in the diagram. However, from this CAM-ERD it is clear that the code and data are critical to the correct operation of the subsystem.

Stage B4

Figure 49, (CAM-ERD) is used together with Table 66 (CAM-C) to create the next level of cause-consequence table as shown in Table 68.

A reformed cause-consequence table is shown below

Table 93 Reformed cause-consequence table

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
201	Controllers differ	The software has latent errors	The software managing the status of each controller has errors which causes the 'view of the railway to differ'	When the controllers swap master function there is a difference causing an unsafe state	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 IEEE1474 	Improbable Probable	Catastrophic	Tolerable Intolerable	<ul style="list-style-type: none"> This is in effect what happened as stated in the evidence. Therefore, the controls are not effective or were not implemented properly.
202	New software unproven	The software has latent errors	The software is changed and novel functionality is introduced	The software malfunctions causing an unsafe state	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 IEEE1474 	Occasional Frequent	Catastrophic	Intolerable	<ul style="list-style-type: none"> This is what happened as stated in the evidence. Therefore, the controls are not effective or were not implemented properly.

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
203	Varying critical new functionality latent errors	Varying critical functionality of software	The design is architected to produce varying functionality of the master, stand-by and warm-stand-by	The change in functionality introduces complexity and potential for latent errors	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 	Remote	Catastrophic	Tolerable	<ul style="list-style-type: none"> The evidence suggests that this was not thoroughly tested
204	System untestable	System too complex	The system is too complex to totally test every variation	Latent errors may be present and fringe functionality uncertain with potentially unsafe state	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 IEEE1474 	Probable Frequent	Catastrophic	Intolerable	<ul style="list-style-type: none"> Because the data space is so large it is impossible to test every combination. As a result, to well use functionality is tested as a subset leaving the more unusual combinations untested. IEEE1474 approach simulation will never cover this ground

Ref	Hazard	Cause	Description	Consequence scenario	Control	Likelihood	Consequence	Risk	Notes
205	Live system has unproven data	Data not proven	Bench testing of the system has not proven the data before live testing and operation	Latent errors with potentially unsafe state	<ul style="list-style-type: none"> Zone controller is designed to comply with EN50128 IEEE1474 	Remote	Catastrophic	Tolerable	<ul style="list-style-type: none"> The evidence is ambiguous on this point. Given that the previous system used data, it is assumed that the static data is reused
206	System does not meet integrity level	System not tested or developed to standard	Development and testing do not follow defined process. Therefore, the probability density of errors is likely to increase	High density of latent errors with potentially unsafe states	<ul style="list-style-type: none"> Zone controller is specified to comply with EN50128 IEEE1474 Company processes 	Improbable Frequent	Catastrophic	Tolerable Intolerable	<ul style="list-style-type: none"> The evidence points to this being the case

Table 93 entries have been examined by the Author and the causal links have been extracted to insert into the developed CAM-C shown in Table 94, which confirms the clear causal links between the controller functions and the system level hazards. Another level could be added if necessary, to probe deeper into the process, but this starts to take the analysis beyond the evidence

available into speculation. Therefore, the analysis is terminated at this level and a mitigation table is populated instead, normally this would all be part of the cause-consequence table; however, the table has been split for clarity.

Table 94 CAM-C for Zone controller - system level hazards

			System level hazards								
			Evidence	Trains off track	Switch setting wrong	Train speeding	Train speeding leaves track	Train outside MA	Faulty MA issued	Zone controller faulty start up	No train detected
				101	102	103	104	105	106	107	108
Controller Hazards	201	Controllers differ	Yes						3	3	
	202	New software unproven	Yes						2	3	
	203	Varying critical new functionality	Yes							3	
	204	System untestable	No						3	3	
	205	Live system has unproven data	No						2		
	206	System does not meet integrity level	Yes						3	3	

Key
3 – Amplifier
2 – Carrier
1 – Resistor
-10 – Terminator

Stage 5 and B4

This stage is used to summarise and present the analysis. Table 91 and Table 93 likelihood and consequence columns have been amended (in red) to indicate the effects of the CAM-C links in the system. These amended values show that some hazards that were initially rated as low risk are in fact much higher.

Table 95 has been created by applying possible mitigations to the analysis, which reduce the severity of the risks to a level where operations could recommence (an objective of this test case).

Table 95 Cause-consequence mitigation table

Ref	Hazard	Cause	Description	Existing Control	Mitigation	Likelihood	Consequence	Risk	Notes
106	Faulty MA issued	Zone controller malfunction	The zone controller issues an MA which is not valid and is in conflict with another train	<ul style="list-style-type: none"> • Zone controller is a high integrity unit and is a 2oo2 	<ul style="list-style-type: none"> • 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> •
107	Zone controller faulty start up	Zone controller malfunction	The zone controller does not initialise and does not operate as per specification as a result fails to keep train separated	<ul style="list-style-type: none"> • Zone controller is a high integrity unit • Zone controller is designed to comply with EN50128, IEEE1474 	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • The reference layout is designed to be simple and have one of everything.

Ref	Hazard	Cause	Description	Existing Control	Mitigation	Likelihood	Consequence	Risk	Notes
201	Controllers differ	The software has latent errors	The software managing the status of each controller has errors which causes the 'view of the railway to differ'	<ul style="list-style-type: none"> • Zone controller is designed to comply with EN50128 IEEE1474 • 	<ul style="list-style-type: none"> • Design to be amended for a consistent view • Logic and hardware to be used to determine status 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • By having a differing model of the railway dependent on status it makes the code more complex and error prone.

Ref	Hazard	Cause	Description	Existing Control	Mitigation	Likelihood	Consequence	Risk	Notes
202	New software unproven	The software has latent errors	The software is changed and novel functionality is introduced	<ul style="list-style-type: none"> • Zone controller is designed to comply with EN50128 IEEE1474 	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout. • All code to be exercised at the modular level. • Critical code to be tested and documented at the system level • Code constructed with defensive programming techniques 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • It is probably not possible to exercise all of the code at the system level because of the complexity. Therefore, module testing is critical. • An effort should be made to thoroughly test critical code with defence in depth.

Ref	Hazard	Cause	Description	Existing Control	Mitigation	Likelihood	Consequence	Risk	Notes
203	Varying critical new functionality	Varying critical functionality of software	The design is architected to produce varying functionality of the master, stand-by and warm-stand-by	<ul style="list-style-type: none"> • Zone controller is designed to comply with EN50128 	<ul style="list-style-type: none"> • Architecture to be modified to produce a consistent set of functionalities. • Logic and hardware to be used to determine status • 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • By providing a consistent functionality it will be easier to test and because of functional simplification latent errors are less likely.
204	System untestable	System too complex	The system is too complex to totally test every variation	<ul style="list-style-type: none"> • Zone controller is designed to comply with EN50128 IEEE1474 	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout • Safety critical system complexity to be reduced as far as possible 	Remote	Catastrophic	Tolerable	<ul style="list-style-type: none"> • Because the data space is so large it is impossible to test every combination. As a result to well use functionality is tested as a subset leaving the more unusual combinations untested. IEEE1474 approach simulation will never cover this ground

Ref	Hazard	Cause	Description	Existing Control	Mitigation	Likelihood	Consequence	Risk	Notes
205	Live system has unproven data	Data not proven	Bench testing of the system has not proven the data before live testing and operation	<ul style="list-style-type: none"> • Zone controller is designed to comply with EN50128 IEEE1474 	<ul style="list-style-type: none"> • Pre-commissioning testing of data • Hand checking of data by competent persons • Data to be simplified to a minimum • Untestable data to be eliminated • Testing of operational scenarios • Comparison of data with the old system 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • Data proving normally relies on process. There is currently no automatic method other than testing for predesignated rules.

Ref	Hazard	Cause	Description	Existing Control	Mitigation	Likelihood	Consequence	Risk	Notes
206	System does not meet integrity level	System not tested or developed to standard	Development and testing do not follow defined process. Therefore, the probability density of errors is likely to increase	<ul style="list-style-type: none"> • Zone controller is specified to comply with EN50128 IEEE1474 • Company processes 	<ul style="list-style-type: none"> • Zone controller to be tested on a reference layout. • All code to be exercised at the modular level. • System functionality to be kept to a minimum • Independent testing by an external body to take place 	Improbable	Catastrophic	Tolerable	<ul style="list-style-type: none"> • The evidence points to this being the case

As can be seen from Table 95, by applying additional mitigations the likelihood is reduced and as a result the risk is reduced to an acceptable level. In essence the mitigations are required as a counter to the non-compliance with process. As has been touched on in Chapter 2 there is currently no method of automatically checking software for practical applications and assurance relies on the application of safety processes.

The effect of the mitigations is summarised in the risk matrices of Table 96 and Table 97.

Table 96 Pre-mitigation risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					202, 204, 206
Probable					106, 107, 201
Occasional					
Remote					203, 205
Improbable					102, 103, 104, 105, 108
Highly Improbable			101		

Table 97 Post-mitigation risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					
Probable					
Occasional					
Remote					203, 204
Improbable					102, 103, 104, 105, 106, 107, 108, 201, 202, 203, 205, 206
Highly Improbable			101		

As can be seen from Table 97 although the potential outcomes of a risk materialising is catastrophic, as would be expected with a safety critical mass-transit control system, the risk is tolerable.

Appendix G - Baildon incident CAM risk analysis

The Author has carried out this analysis using CAM as part of a case study to compare using output and comparing it with the publicly available information from an RAIB investigation report (Rail Accident Investigation Branch, 2017), which has been produced to describe their analysis. Appendix D contains the particulars of the incident. Baildon is a near-miss incident where had events turned out slightly differently i.e., the rails gave way, fatalities could have happened.

The analysis is simplified to enable rapid development of the method, given the limited detail available, and therefore hazard identification has been limited in this case to the essential facts.

Appendix Contents

G1 Assessment of risk	397
G2 Method used	399
G3 Analysis	400
G3.1 FMEA	404

G3.2 CAM Combinator

413

G3.3 Combined system cause consequence table

419

G3.4 Summarised risk matrix

422

G1 Assessment of risk

For this test case study, a semi-qualitative method of assessing risk has been used based on EN50126 (CENELEC, 2017), shown in Table 98, as a calibrated likelihood-consequence table to perform a qualitative risk assessment evaluation. The Author has scaled the frequency assuming a system life span of 20 years, on the basis that process and operating practices are unlikely to remain unaltered beyond that point.

This matrix is used to determine the acceptability of the risk using values that align with the ORR guidance (Office of Rail and Road, 2018). The green areas are 'broadly acceptable' and require no further mitigation, yellow areas are 'tolerable' and require mitigation to a level that is ALARP, and the red areas are 'intolerable' indicating that they cannot be accepted.

Table 98 Risk matrix formulated from (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic	
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable	<1yr
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable	<2yrs
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable	<5yrs
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable	<10yrs
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	<20yrs
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	≥20yrs

G2 Method used

The analysis method used is as explained in Chapter 6, and documented in Appendix J (CAM user instructions) Section J2 and labelled as CAM-FN (Forward New/novel/modified analysis). The Author has decided for the purposes of this test case that the CAM-FN variant is more appropriate than the accident variants because the objective is to see if a CAM analysis produces a set of outputs rather than attempt to trace the causes from an incident.

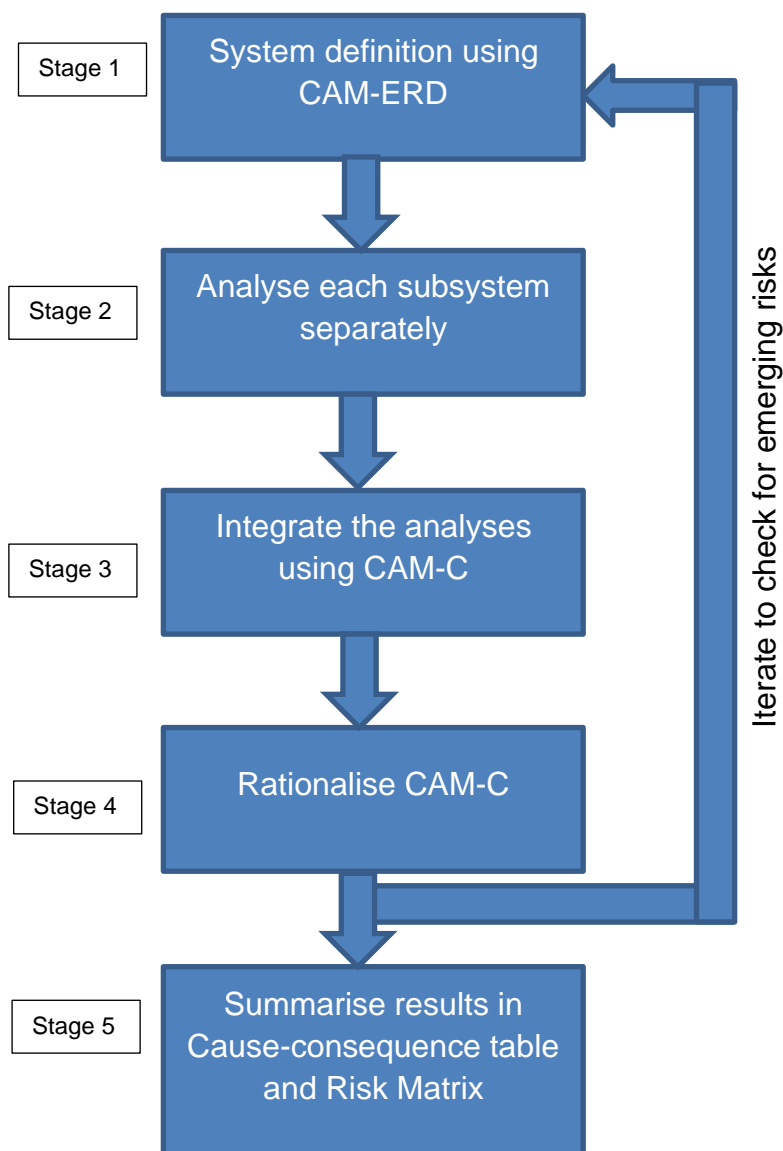


Figure 50 CAM_FN process reproduced from Appendix J

For this analysis FMEA has been selected as the method for the subsystem analysis because it was found to be the most popular from the industry analysis in Chapter 4.

G3 Analysis

The Author has undertaken this CAM risk analysis in accordance with the CAM user instructions contained in Appendix J Section J2. The Baildon incident details referred to in this analysis are taken from Appendix D. This appendix is used to maintain a consistent set of facts between the analyses in the resulting case study.

CAM Stage 1

The first task is functional decomposition as described by Rasmussen (1997) by structural systems and behavioural flow. This is performed using the CAM-ERD as described in Stage 1 of Appendix J. Table 99 is used as an initial listing of the system elements before creating the CAM-ERD to facilitate the translation of facts from Appendix D to this analysis.

Table 99 Systems table

Main sub-system or system	Components/actors	Comments
Rail line – single-line	<ul style="list-style-type: none"> • Rails • Concrete sleepers 	
Ground	<ul style="list-style-type: none"> • Single-sided embankment 	There is a single-sided embankment, but at some point, along the route there is a cutting.

Signalling	<ul style="list-style-type: none"> • Track circuit block 	<p>Connected to York signalling centre.</p> <p>Will only change state if the current flow is broken (i.e. the rail breaks)</p>
Environment	<ul style="list-style-type: none"> • Water flow • Flood water 	Water flows from the drainage area
Beck	<ul style="list-style-type: none"> • Pipes inserted to reduce diameter by 1/3 	
Culvert	<ul style="list-style-type: none"> • Inspection chambers 	Connected to Beck.
People	<ul style="list-style-type: none"> • Controllers (York SCC) • Signaller • Mobile Operations Manager (MOM) • Track Engineer (TE) 	The MOM and TE inspected the track.

Figure 51 is the CAM-ERD for the Baildon incident. Subsystems are represented by circles, parts by rectangles and the point of harm by a red triangle. The relationships are represented by arrows. These relationships normally show the flow of risks, but they can also show other labels to assist in the understanding of the system to be analysed.

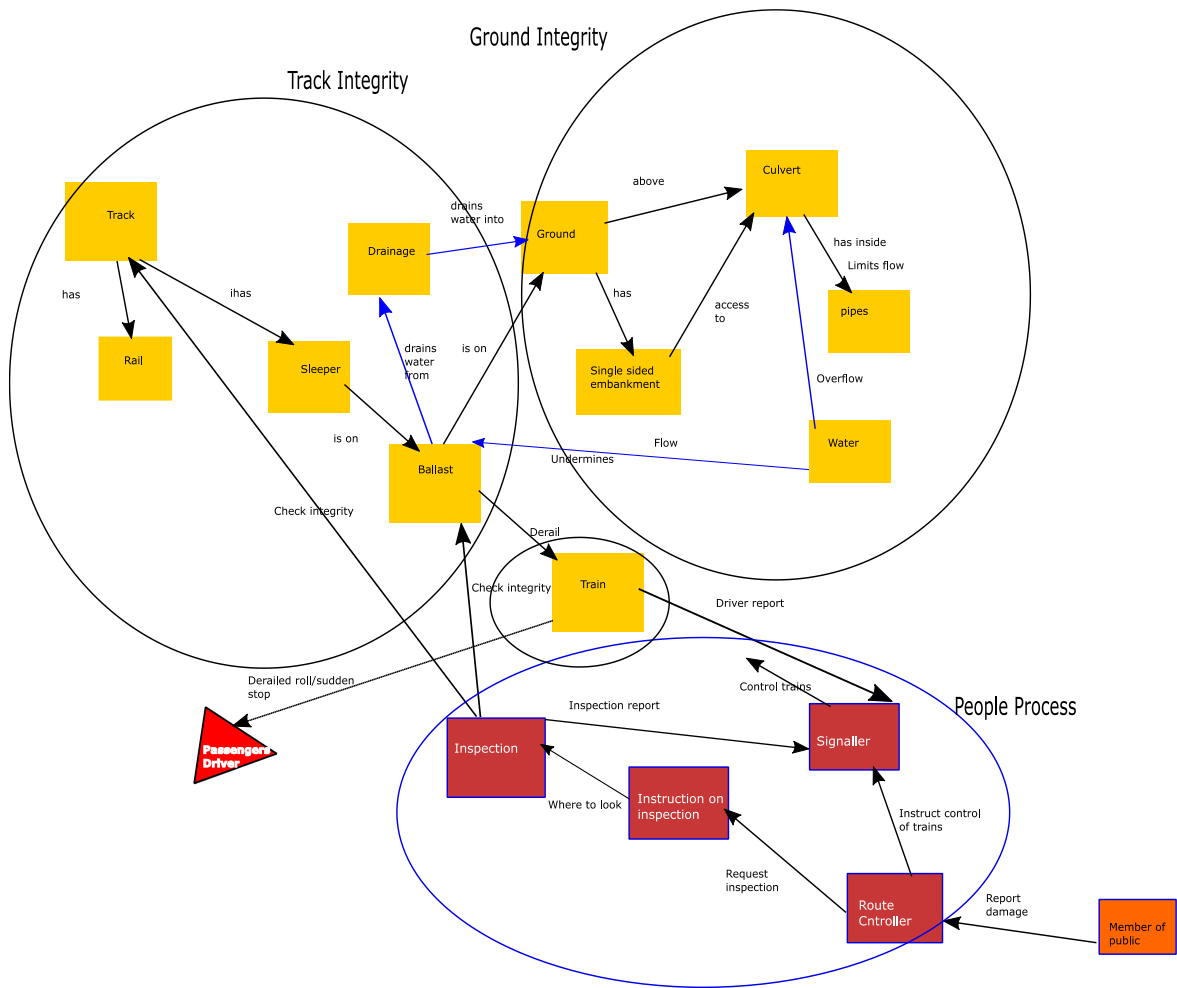


Figure 51 Baildon CAM-ERD

Figure 51 shows that there are two key physical systems where safety is dependent on the integrity of the physical system.

The drainage subsystem is comprised of the ballast and track bed substrate and not an actual drainage pipe. The porous nature allows the water to soak away into the ground under normal conditions.

Notes

Notes on flow through pipes

Keynote: volume is controlled by the diameter of the pipes as noted in

<https://www.quora.com/What-is-the-relationship-between-pressure-differential->

and-the-amount-of-fluid-that-flows-through-a-pipe (Thigle, 2013), resulting in a relationship of volume proportional to the cross-sectional area and velocity of the fluid which is derived from Bernoulli's equation.

Therefore, by reducing the diameter of the pipes, the speed is increased, and the pressure is also reduced. It will act to lower the pressure and therefore stop the inspection holes from overflowing although this might cause safety issues elsewhere in a residential area, due to a reduced ability to drain the catchment area.

G3.1 FMEA

CAM-Stage 2 Subsystem analysis

The selected tool for the CAM stage 2 subsystem analyses is FMEA.

A desktop FMEA analysis has been conducted using EN60821 (CENELEC, 2006) and Anleitner (2010) and tailored to a safety application in a similar way to Mohr (2002) presented to the University of Wisconsin-Madison. The approach is to treat the systems as performing a function and then to document the failure of the function. A high detection number of 10 indicates that it will be easy to detect and prevent through the applied controls. Conversely, a low score indicates that the failure is difficult to detect and therefore may be latent. The classification is S for a significant function failure and C, for a critical failure where there is a direct safety implication. Classification conversions, if necessary, from S to C are performed by adjusting the occurrence to reflect that not every failure will result in a safety event as articulated by Lepmets (2017). Also, consideration will be taken of the effect of detection and controls when setting the occurrence in the case of a safety classification. The RPN field is not considered appropriate for this particular application.

The scale for severity and conversion of the frequency to a scale used in the risk matrix are given in Table 100 and Table 101 below, in preference to the normal 10-point scale.

Table 100 Scaling table for occurrence formulated from (CENELEC, 2017)

Occurrence Category	Value	Definition
Frequent	6	Less than a year
Probable	5	Less than 2 years
Occasional	4	Less than 5 years
Rare	3	Less than 10 years
Improbable	2	Less than 20 years
Highly Improbable	1	Greater or equal to 20 years

Table 101 Scaling table for the severity formulated from (CENELEC, 2017)

Category	Value	Safety Definition	Equipment failure definition
Catastrophic	5	Multiple fatalities	Multiple systems loss
Critical	4	Fatality/multiple major injuries	Major loss of system
Major	3	Life changing injury	Severe systems damage
Marginal	2	Injury	Minor systems damage
Insignificant	1	No material harm	

Table 102 FMEA for ground integrity (culvert and environment)

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
101	Culvert	Water flow	Failure during operation	Blocked	No water flow		2	S	Large amount of debris	1yr	Sieves on pipework	Inspection and surveys	10		There may be water overflow further upstream. The direction of the water will be dependent on the lie of the land, could flow onto railway land.		5
102	Culvert	Water flow	Failure during operation	Blocked	reduced water flow		2	S	Small amount of debris	6m	Sieves on pipework	Inspection and surveys	5		The water may overflow further upstream and flow onto railway land.	3	5
103	Culvert	Support the ground above	Failure during operation	Structural collapse	Land subsides	Possible derailment and injuries	4	C	Too much weight on the structure	20yr	Design codes	Reports from railway	5		The culvert will cease functioning	1	1

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
104	Culvert	Water volume flow	Failure during operation	Water leaks out of inspection manholes	water flows down the embankment	Water lows along the railway	2	S	Pressure too high as a result of too higher volume	20yr	Control of pressure and flow volume	Reports from the surrounding area and calculations	5		The pressure forces the water to rise up the inspection manholes and pop the covers. If this happens, water flows down the embankment and over the railway.	2	3
105	Pipes	Water flow volume	Failure during operation	Flow not high enough	Head builds		3	S	Too much water	10yr	Reduction in pipe size	Flood reports	5		It could cause the water to overflow upstream and will limit the volume of water. Equations show that the volume is controlled by pipe diameter. Also, the head will increase the pressure. However, this has happened twice in over 50yrs, therefore, does not happen often	2	2, 3, 6

Table 103 FMEA for track integrity

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
201	Ballast	Support sleepers	Failure during operation	Falls away	Sleepers unsupported	Possible derailment and injuries	4	C	Ground collapse	10yr	Providing support for ground	Inspection and reports	3		Overall track beds are stable structures with life spans of the order of 60 yrs. It is assumed that some maintenance will have to take place every 10 yrs to keep the condition If the sleepers are left in mid-air, a train will cause the rails to bend and possibly cause a train to overturn or derail	21, 23	
202	Ballast	Support sleepers	Failure during operation	Washed away	Sleepers unsupported	Possible derailment and injuries	4	C	Strong water flow	10yrs 20yrs	Keep water in drains or fit retaining mesh to the ballast. Also, GE/RT8000-M3 stopping trains	Inspection and reports	3		If the sleepers are left in mid-air, a train will cause the rails to bend and possibly cause a train to overturn or derail. Sleepers use ballast to tied the railway to the ground. The rule book anticipates this problem and is a control. This reduces the safety incidence to an estimated 20 yrs, even if the ballast is washed away.	2, 5, 10, 14, 15, 21	

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
203	Sleepers	Keep rails in place	Failure during operation	Moves	Rails move	Possible derailment and injuries	4	C	No ballast	10yrs	Retain ballast	Inspection and reports	3		Overall track beds are stable structures with life spans of the order of 60 yrs. It is assumed that some maintenance will have to take place every 10 yrs to keep the condition. If the sleepers move, the rails will move. If the rails move, the train could derail. It is unlikely that they will move laterally because they are tied by the rails and other sleepers. But it would be free to move vertically. However, the rule book will act to mitigate the safety issue of trains using the damaged track	21, 23	

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
204	Sleepers	Support load	Failure during operation	Sleeper not supported	Rails dip	Possible derailment and injuries	4	C	No ballast	10yr	Retain ballast	Inspection and reports	3		Overall track beds are stable structures with life spans of the order of 60 yrs. It is assumed that some maintenance will have to take place every 10 yrs to keep the condition If the sleepers are left in mid-air, a train will cause the rails to bend and possibly cause a train to overturn or derail	21	
205	Drainage	Drain water from ballast	Failure during operation	Overwhelmed	Drainage waterlogged	Railway flooded; Rails underwater	4	C	Too much water	5yr 10yrs	Limit volume of water Also, GE/RT8000-M3 stopping trains	Inspection reports and design	2		If the drainage is overwhelmed water may flow down the railway or form a stagnant pool. Only if there is a strong flow will it wash the ballast away. The rule book anticipates this problem and is a control. It reduces the safety incidence to an estimated 10 yrs, even if the ballast is washed away.	19	5, 6

Table 104 FMEA for trains

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
301	Train	Move on rails	Failure during operation	Derailment	Fatality, injuries	Fatality, injuries	4	C	Rails fail to support train	20yrs	Signalling	Inspection and reports	5		There are regular derailments; however, these are mainly in sidings. On the mainline this is an unusual event. If the train derails, there is a risk that there could be casualties	14, 21	

Table 105 FMEA for people process

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
401	Mtce Engineer	Spot faults	Failure during operation	Failure to a spot fault	Degraded railway	Possible derailment with Injuries	4	C	Missed fault	5yrs	Instructions Training	Subsequent inspections Reports by others	2		The Track Technician is a maintenance engineer. The report states that the inspection did not go far enough. Normally there are contingencies built into engineering standards. However, in this case, there was a failure. Overall, it is estimated that it would occur 5yrs	8, 17, 20	

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
402	MoM	Spot faults	Failure during operation	Failure to a spot fault	Degraded railway	Possible derailment with Injuries	4	C	Missed fault	5yr	Instructions Local knowledge	Subsequent inspections Reports by others	2		The MOM went to the wrong place and could not see the faulty stretch. However, in many cases the omissions are not critical. There is likely to be a smaller proportion that is critical without a chance to correct the error.	4, 8, 18	
403	MoM	Spot faults	Failure during operation	Failure to a spot fault	Degraded railway	Possible derailment with Injuries	4	C	No access	10yrs	Certification, supervision and alternate MOMs	Health reporting	8		The controller was aware of the limitation.	2	
404	Signaller	Stop trains	Failure to operate at prescribed time	Not stop trains	Route set for trains onto damaged line	Possible derailment with Injuries	4	C	Not informed	10yrs	Training Supervision	Monitoring Driver reports	2		The signaller not informed until after the first train and unaware that fault persisted	5, 6, 22	
405	Signaller	Stop trains	Failure to operate at the prescribed time	Not stop trains	Route set for trains onto the damaged line	Possible derailment with Injuries	4	C	Incorrect information	10yrs	Training inspection of the line by driver/other	Monitoring Driver reports	2		In this case, the technician stated it was safe. In addition, the initial fault was reported as flooding.	20	
406	Route controller	Receive an emergency message	Failure to operate at the prescribed time	Not act on the message	Message or information lost	Possible derailment with Injuries	4	C	Incorrect decision	10yrs	Training Supervision	Monitoring	2		The second call to the controller resulted in no action because he thought it was under control.	7	
407	Route controller	Instruct signaller	Failure during operation	Fail to give clear instruction	Confusion and delay in getting the signaller to act	Possible derailment with Injuries	4	C	Mis-understand	10yrs	1 Registers 2 Safety critical Comms	Monitoring via voice recorder	2		This happened via the signalling Mgr, eventually. There are examples of lapses, but the consequence is averted by the driver or signaller	5, 16, 22	

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
408	Route controller	Receive emergency message	Failure during operation	Fail to interpret the message correctly	Confusion and delay	Possible derailment with Injuries	4	C	Limited local knowledge	5yrs	1 Training	Monitoring via voice recorder	2		The misinterpretation of the initial message from the public led to searching in the wrong place for the fault and ensuing confusion and late realisation of what and where the problem was.	5, 11, 16	

G3.2 CAM Combinator

CAM-Stage 3 – CAM-C

The CAM Combinator (CAM-C) is laid out in Table 106. The convention adopted is input columns and outputs are rows. This convention is interpreted as the columns acting as causes for the hazard indicated in the rows. Using CAM-C, a chain of events can be traced through the system. This particular CAM-C has been formed by taking the failures from the FMEA entries to create the single view for the whole system and then convert this to a cause-consequence table later in the process, as described in Appendix J. The CAM-C entries have been organised by grouping the failures around subsystems as indicated in the CAM-ERD. The individual entries can be traced back to the FMEAs through the 'Ref' entry, e.g., 101.

Key for

combinator 3 - amplifier

2 - carrier

1 - resistor

-10 - terminator



post event mitigation

Table 106 Baildon CAM-C

			Culvert		Pipes	Ballast	Sleepers	Drain	Train	Mtce Eng	MoM	signaller	Route controller							
			101 102	103	104	105	201	202	203	204	205	301	401	402	403	404	405	406	407	408
Culvert																				
	101	Blocked																		
	102																			
	103	Structural collapse																		
	104	Water leaks out of manholes				3														
Pipes																				
	105	Flow not enough																		
Ballast																				
	201	Fallen away																		
	202	Washed away								1										
Sleepers																				
	203	Moved		2																
	204	Sleeper not supported					3	3												
Drainage																				
	205	Overwhelmed			2															
Train																				
	301	Derailment						3	3							2	3			
Mtce Eng																				
	401	Failure to spot fault																		2
MoM																				
	402	Failure to spot fault																		2
	403	Failure to spot fault no access																		
signaller																				
	404	Stop trains																		
	405	Stop trains wrong info										3	2							3
Route controller																				
	406	Stop trains																		
	407	Fail to give clear instruction																		
	408	Fail to interpret message correctly																	2	

A post-event mitigation is defined as an action that takes place after the damage has occurred and the hazard exists, but before further avoidable triggers have happened, leading to a potential incident. Post-event mitigations are typically actions taken by people using processes to stop trains and limit the time at risk and the number of additional events.

As can be seen, the key physical subsystem appears to be the sleepers. If they move or are unsupported, there is a risk of a derailment. The source of the movement leads back to a structural collapse or flooding from an overflow of the culvert. What is also interesting is that the people interventions post-event has no effect on the initial near-miss, although they do affect the subsequent risk for follow on trains. This is because the reports that trigger a people intervention occurred after the physical incident happened. The other failures do not appear to affect the railway.

Rationalisation CAM-Stage 4

Items 101, 102 and 103 do not feature because although there is a potential risk they did not contribute to the incident as defined by the CAM-ERD point of harm and are left blank indicating there is no link. Similarly, 201 did not feature in the accident and is left blank, because this risk is concerned with a structural failure which did not happen. There is no link from 404 and is left blank because the lack of information occurred after the initial event to stop the first train. The overall system represents a linear progression. Two links can be rationalised as an internal link, 403 to 402 and 407 to 408. Link 403 is a contributory factor to 402 the missed inspection. Likewise, 407 is concerned with the controller's impression that the incident was under control and is a form of confusion. The rationalisation is improved by, selecting 104 as the summarisation of 104 and 105. It represents the joint cause of the flood plus the manholes, which taken together is regarded as a design cause. Item 204 could be argued to be a version of 203 because the sleepers are tied to the rails, as identified in Appendix D (fact 24). However, there could be movement in the sleepers as well as being unable to support the load (Appendix D fact 25); on that basis, it has been left in the analysis.

The rationalisation of intermediate links has been left to later in the process, as a separate demonstration

Output CAM-Stage 5

Table 107 is a combined FMEA by collecting together items identified as either a carrier, amplifier or resistor. The frequencies have been adjusted (in red) for summarised items where the lower level was an amplifier or resistor, following the process described in Appendix J. In addition, a column has been appended to the right to indicate the level increase or decrease when the cause is referred to the system level. A value of 1 is a one-level increase when the overall value is calculated. Items identified as an amplifier have had the frequency adjusted to reflect the increased risk

in this configuration of the total system. In this case, a doubling of the frequency was judged appropriate. The frequency was chosen because the consequence increase cannot be justified in this particular case.

Table 107 System-level FMEA table

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Secondary hazard	Increase at sys level
104	Culvert	Water volume flow	Failure during operation	Water flows out of inspection manholes	water flows down the embankment	High water flow along the railway	2	S	Pressure too high. Pipes contribute to pressure	20yrs 10yrs	Control of pressure and flow volume. Also, provide run-off drainage	Reports from the surrounding area and calculations	5		The pressure forces the water to rise up the inspection manholes and pop the covers. Note that there was a recommendation previously to divert the overflow into soak drainage. However, there is nothing which makes it an issue. Combined effect from 105		1
202	Ballast	Support sleepers	Failure during operation	Washed away	Sleepers unsupported	Possible derailment and injuries	4	C	Strong water flow	20yrs	Keep water in drains or fit retaining mesh to the ballast. Also, GE/RT8000-M3 stopping trains	Inspection and reports	3		If the sleepers are left in mid-air, a train will cause the rails to bend and possibly cause a train to overturn or derail. There is a rule book instruction to stop trains when there is a flood.		2
203	Sleepers	Keep rails in place	Failure during operation	Moves	Rails move	Possible derailment and injuries	4	C	No ballast	10yrs	Retain ballast	Inspection and reports	3		If the rails move the train could derail		1

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Secondary hazard	Increase at sys level
204	Sleepers	Support load	Failure during operation	Sleeper not supported	Rails dip	Possible derailment and injuries	4	C	No ballast	10yr	Retain ballast	Inspection and reports	3		If the sleepers are left in mid-air, a train will cause the rails to bend and possibly cause a train to overturn or derail.		1
205	Drainage	Drain water from ballast	Failure during operation	Overwhelmed	Drainage waterlogged	Railway flooded; Rails underwater	4	C	Too much water	10yrs	Limit volume of water Also, GE/RT8000-M3 stopping trains	Inspection reports and design	2		If the drainage is overwhelmed, water will flow down the railway and may wash the ballast away. The rule book anticipates this problem and is a control. This control reduces the safety incidence to an estimated 5 yrs, even if the ballast is washed away.		1
301	Train	Move on rails	Failure during operation	Derailment	Fatality, injuries	Fatality, injuries	4	C	Rails fail to support train	20yrs	Signalling and track inspection	Inspection and reports	5		If the train derails, there is a risk that there could be casualties.		0
401	Mtce Engineer	Spot faults	Failure during operation	Failure to the spot fault	Degraded railway	Possible derailment with Injuries	4	C	Missed fault	5yrs	Instructions Training	Subsequent inspections Reports by others plus contingency in design	2			Yes	1
402	MoM	Spot faults	Failure during operation	Failure to the spot fault	Degraded railway	Possible derailment with Injuries	4	C	Missed fault	5yr	Instructions Local knowledge	Subsequent inspections Reports by others	2			Yes	0

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects (local)	Potential failure effects (system)	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Secondary hazard	Increase at sys level
405	Signaller	Stop trains	Failure to operate at the prescribed time	Not stop trains	Route set for trains onto the damaged line	Possible derailment with Injuries	4	C	Incorrect information	10yrs	Training inspection of the line by driver/other	Monitoring Driver reports	2		In this case, the technician stated it was safe	Yes	0
406	Route controller	Receive an emergency message	Failure to operate at the prescribed time	Not act on the message	Message or information lost	Possible derailment with Injuries	4	C	Incorrect decision	10yrs	Training Supervision	Monitoring	2			Yes	1
408	Route controller	Receive emergency message	Failure during operation	Fail to interpret the message correctly	Confusion and delay	Possible derailment with Injuries	4	C	Limited local knowledge	5yrs	1 Training	Monitoring via voice recorder	2		The misinterpretation of the initial message from the public led to searching in the wrong place for the fault and ensuing confusion and late realisation of what and where the problem was.	Yes	1

Comments on the alignment of combined System FMEA with the CAM-C

1. Item 204 in CAM-C indicates two physical causes summarised as a lack of support for the sleepers due to a lack of ballast. Either the ballast has been washed away, or it has fallen away. In this case CAM-C has been interpreted to use only 202, which in this case is the specific cause, using information from Appendix D.
2. Item 301 in the CAM-C indicates two physical causes that cause the rails to fail to support the train that are listed within the CAM-C and therefore the FMEA appears to be well aligned.
3. The people item interactions are more complex, reflecting that people are more flexible in an overall system and can be used to fill gaps in the physical design. The inputs from items 401 and 402 reflect that the Maintenance Engineer and Mobile Operations Manager have some parallel duties and could have interceded to identify that the track is not intact. Likewise, if they are incorrectly told what to do, then they will fail as identified in the interaction with the Route Controller. Finally, the CAM-C indicates that all the key people had a chance of preventing the follow-on incidents had they been aware earlier and acted without error, but they could not have prevented the initial incident unless they had prior knowledge.

G3.3 Combined system cause consequence table

As highlighted by Lepmets (2017), the common currency between an FMEA and hazard analysis is the expression of the cause. The consequence and likelihood are influenced by the FMEA. Where the failure is denoted as a safety failure, the consequence will be the same. The cause-consequence table is drawn together from the system level FMEA and developed into a risk expression through the application of Table 98 defined in G1 Assessment of risk

Failures in the FMEA create potential hazardous states as noted by Lepmets (2017); however, these need to be recast to match the system configuration. Hazards are created from the CAM-ERD and CAM-C. From those diagrams, it is clear that the sleepers and track support are a key state, the controller interface (with the public) and handling of information and the flow of water. Also, the interaction between the train and track is a key state.

Table 108 Cause-consequence table

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Consequence	Control	Evaluation type	Likelihood	Consequence	Risk
104	Manhole leak	High Water flow	Pipes	Pipes do not allow enough flow causing pressure rise and water to burst out of manhole covers and flows at a high rate	Water flows onto the railway	Railway track bed is flooded, and water is fast flowing washing out ballast causing a derailment as injuries	Injuries and possible fatalities	Design control of flow and pressure	Risk Estimation	Occasional	Catastrophic	Intolerable
202	Ballast removal	Track unstable	Ballast washed away	The ballast is not fixed and is washed away by a flow of water	The track is unsupported and becomes unstable. It is unable to support a train	Track moves and derails a train causing injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable
203	Sleepers move	Track unstable	Sleepers moved	The sleepers supporting the rails move, which causes the alignment to change	Train experiences a discontinuity	Track moves and derails a train causing injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable
204	Sleeper not supported	Track unstable	Sleeper unsupported	The sleeper is unsupported, which allows vertical movement when a train is present. Often	Rail dips and train not supported	Track moves and derails a train causing injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Consequence	Control	Evaluation type	Likelihood	Consequence	Risk
				it results only in a rough ride rather than more severe consequences								
205	Track flooded	Track unstable	Drainage overwhelmed	The drainage (normal soak away) cannot cope with the volume of water and water flows along the track	The force of the flow removes ballast and distorts track causing a derailment	The derailment of the train causes injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable
301	Train derails	Track in poor condition	Train does not follow rails	The train comes off the rails because it cannot follow the track which is in poor condition	The Train comes off the track, and people are injured because the train rolls	The derailment of the train causes injuries	Injuries and possible fatalities	Signalling and track inspection	Risk Estimation	Highly improbable	Catastrophic	Tolerable
401	Track fault unseen by MOM	Track fault undetected	MOM did not spot the fault	The MOM did not spot the track fault on inspection	Train unable to stay on track	The derailment of the train causes injuries	Injuries and possible fatalities	Track inspection process	Risk Estimation	Rare	Catastrophic	Tolerable
402	Track fault unseen by engineer	Track fault undetected	TE did not spot the fault	The TE did not spot the track fault on inspection	Train unable to stay on track	The derailment of the train causes injuries	Injuries and possible fatalities	Track inspection process	Risk Estimation	Rare	Catastrophic	Tolerable
405	Trains not stopped	Line open	Signaller has incorrect information	The signaller is fed incorrect information and does not stop trains	Train unable to stay on track	Trains are routed along the damaged line and derail	Injuries and possible fatalities	Rule Book/ inspection by driver or another	Risk Estimation	Improbable	Catastrophic	Tolerable
406	Emergency message not actioned	Control actions ineffective	Lack of situational understanding	The controller dealing with the message is confused	Train unable to stay on track	The information is lost from the system and trains are allowed to use the damaged line	Injuries and possible fatalities	Training and supervision	Risk Estimation	Rare	Catastrophic	Tolerable

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Consequence	Control	Evaluation type	Likelihood	Consequence	Risk
408	Emergency message misunderstood	Control actions ineffective	Limited local knowledge	The controller does not appreciate the actual location of the reported fault	Train unable to stay on track	The confusion leads to delay and inaction. Trains are allowed to use the damaged line	Injuries and possible fatalities	Training and voice recorders	Risk Estimation	Occasional	Catastrophic	Intolerable

G3.4 Summarised risk matrix

A risk matrix has been drawn up from the cause-consequence table. This illustrates the effect of simplification inherent in CAM and points to the culvert as an intolerable risk (104). The secondary risk of ‘confusion’ (408) is also highlighted as an intolerable key risk. As, indicated by RAIB this ‘confusion’ is a symptom of a lack of clear processes and responsibility. The large number of risks that are in the ‘catastrophic’ column of the matrix is, in the Author’s experience, symptomatic of a system that is out of control.

Table 109 Baildon risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					
Probable					
Occasional					104, 408
Rare					202, 203, 204, 205, 401, 402, 406,
Improbable					405
Highly Improbable					301

As can be seen, the analysis points to two intolerable risks one concerned with the manhole, and one associated with the confusion with the controllers.

CAM-C has been used to differentiate secondary and primary risks. Primary risks in this case are those that would have prevented the initial physical event happening if they had been addressed; while secondary risks are those that affect the post event outcomes. Those risks that arose after the initial event were coloured beige in the CAM-C. These were identified from the ‘facts’ in Appendix D. In particular, the people risks are determined to be secondary because their intervention only occurred after the initial event. Therefore, there are six primary

risks (104, 202, 203, 204, 205), all these are physical, and one is intolerable (104). This outcome suggests that the recommendations from the official report should have placed greater emphasis on the physical shortcomings rather than the people. From a CAM process perspective this differentiation shows the flexibility of CAM-C.

As indicated in the rationalisation stage of the process a further level of rationalisation is possible by removing the redundant intermediate links using the process described in Appendix J. The result shows that there are three root causes.

Table 110 Baildon rationalised risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent	Yellow	Red	Red	Red	Red
Probable	Yellow	Yellow	Red	Red	Red
Occasional	Yellow	Yellow	Yellow	Yellow	Red (104, 408)
Rare	Green	Green	Yellow	Yellow	Yellow (406)
Improbable	Green	Green	Green	Yellow	Yellow
Highly Improbable	Green	Green	Green	Yellow	Yellow

Appendix H - Baildon incident STAMP STPA risk analysis

This is a STAMP analysis conducted as part of a case study carried out to benchmark the CAM analysis method using the publicly available information from an RAIB investigation report (Rail Accident Investigation Branch, 2017), which has been created from their analysis. The particulars of the incident are contained in Appendix D. The analysis method chosen is representative of a sociotechnical way of carrying out system safety risk analysis. The outcome is used to compare and contrast with other methods of analysis including CAM.

The analysis has been simplified to enable a rapid development of the method, given the limited detail available, and therefore hazard identification has been limited in this case to the essential facts.

Appendix Contents

H1 Assessment of risk	425
H2 Method used	425
H3 Analysis	427

H3.1 stage 1 – purpose of the analysis	
H3.2 Stage 2 – Model the control structure	427
H3.3 Stage 3 - Identify unsafe control actions (UCAs)	429
H3.4 Stage 4 - Identify loss scenarios	434
H3.5 Analysis interpretation	447
	485

H1 Assessment of risk

STPA and STAMP do not refer to a method of assessing risk with reference to a calibrated reference.

H2 Method used

A variant of STAMP, System Theoretic Process Analysis (STPA) , which is a general analysis variant as described in Leveson (2011) has been selected. It is documented as a nine-step process which is summarised below:

1. Identify the potential inadequate control of the system that could lead to a hazardous state;
2. Check if safety constraints have not been met because:
 - a. A control action is not provided or followed
 - b. An unsafe control action is implemented
 - c. A safe control action is provided at the wrong time or in the wrong sequence

- d. A safe control action carries on for too long or is stopped too soon;
3. Establish how each hazardous control action identified above could happen
- a. Examine how each part of the control loop could cause the action. Evaluate existing control measures
 - b. Consider how design controls can degrade over time
 - i. Including management of change
 - ii. Unplanned change
 - iii. Use incident analysis to trace through to the system design

The objective is to identify the hazards and safety constraints that if violated could lead to an accident.

Tutorials produced by MIT (Thomas, 2013), (Leveson and Thomas, 2018b) and (Fleming, 2013).

Primarily the 2018 handbook (Leveson and Thomas, 2018b) ,has been followed for this exercise as the most up to date version of the process. This has four stages listed as:

1. Define the purpose of the analysis
2. Model the control structure
3. Identify unsafe control actions
4. Identify loss scenarios

Templates have been used from Leveson and Thomas (2018b) as necessary in this appendix. The analysis is supplemented by the other tutorial publications where the handbook is not clear. The process described in the handbook is designed to create a number of outputs in the analysis which are linked as illustrated in Figure 52. These output headings are used to define the analysis output sections and how they are linked.

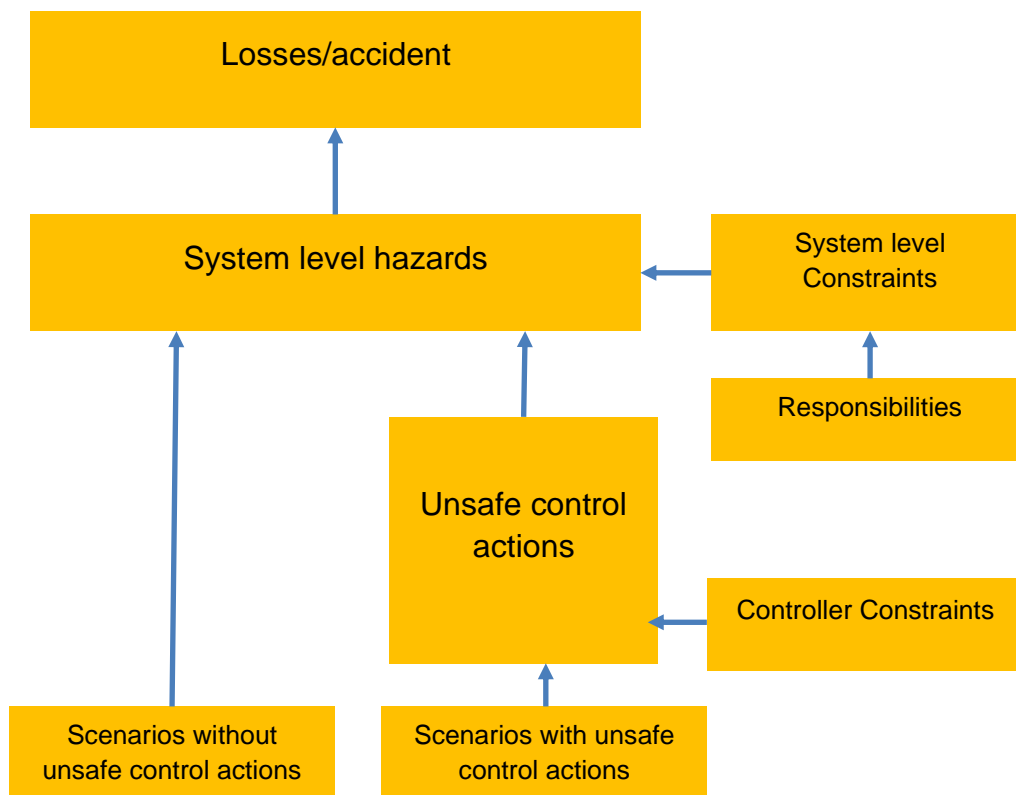


Figure 52 STPA outputs of analysis (Leveson and Thomas, 2018b)

H3 Analysis

The analysis relies on the facts established in the RAIB report through its investigation. The particulars are contained in Appendix D.

H3.1 stage 1 – purpose of the analysis

The incident is taken as trains were permitted to traverse the unsupported track on a section of line. The resulting accidents are determined as:

A1: train falls off line injuring passengers rolling down embankment.

A2: train is derailed injuring passengers.

The system level hazards are identified.

It is assumed that the RAIB report contains the immediate events and these are used to identify the main hazards:

H1: Damaged line cannot support train weight – linked to A1 and A2

H2: Damaged line open to traffic – linked to A1 and A2

H3: Train does not follow commands – linked to A2

Sub hazards for H1

H1.1: Line deformed beyond train gauge

H1.2: Line support missing

A Hazard in STPA is defined as a state where under worst case conditions would lead to an accident. Under this criterion It is debatable whether a hazard of “line flooded” should be included. As a state it is not dangerous. It is only deemed to be dangerous because ballast could be washed away as a result. This would mean that state H1 would be reached if that occurred. If H1 was not reached, there may be uncertainty about the state of the track bed but logically it would still be intact. Consequently, it has been decided not to include it on the grounds that H1 would lead to an accident (potentially), but a line flooded would not except under specific circumstances included in H1.

The safety constraints are identified.

The system level safety constraints determined from the hazards are:

SC1: The trains must not operate over damaged track structures -linked to H1, H2

SC2: The track structures must withstand environmental conditions -linked to H1,
H1.2

SC3: The line must be closed if damage occurs -linked to H2

SC4: Train must stop before damage on the line -linked to H1

SC5: Line must be inspected regularly – linked to H2

SC6: Line must be closed if damage reported – linked to H2

SC7: Line must support weight of train – linked to H1, H1.1 and H1.2

SC8: Train must only operate over authorised routes – linked to H2

SC9: Train must not operate over flooded line – linked to H1.2

H3.2 Stage 2 – Model the control structure

The high-level safety control structure constructed from the RAIB report is as follows:

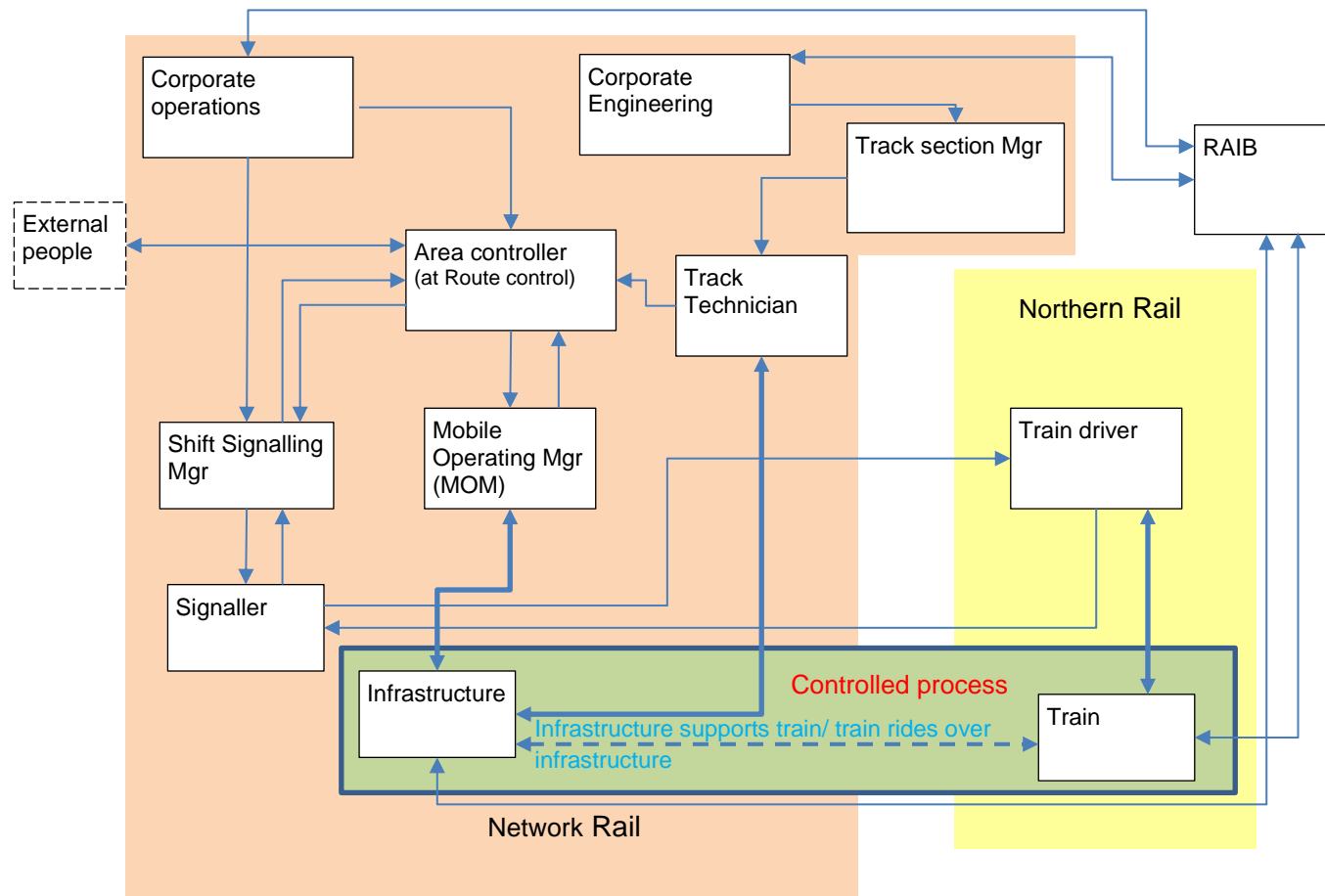


Figure 53 Initial control structure

Responsibilities developed from initial control structure:

Track bed

R1: to support the track – linked to SC7

Drainage

R2: to keep track clear of water – linked to SC9

Track section Mgr

R3: issue standards maintenance and inspection schedules to maintain line in good order – linked to SC5, SC2

Track technician

R4: Inspect and maintain the track – linked to SC5, SC9

R5: report findings and work completed – linked to SC5, SC9

Mobile Operations Mgr

R6: Investigate incidents as requested and report findings – linked to SC9, SC6

Area controller

R7: Respond to calls reporting damage to infrastructure – linked to SC6, SC3

R8: Instruct that line is closed if damaged – linked to SC1, SC3, and SC6

Signalling Manager

R9: Maintain an overview of train movements and control of signallers – linked to SC8

R10: Pass instructions from route control to the signaller – linked to SC3

Signaller

R11: enforce rule book regulations about water on the line – linked to SC9

R12: close the line if there is reason to believe it is damaged – linked to SC3, SC9, and SC6

R13: Control the movement of trains – linked to SC8

R14: Close flooded line to trains – linked to SC9.

Corporate operations

R15: Create distribute and enforce standards including the industry Rule Book – linked to SC9, and SC8

Corporate engineering

R16: Create distribute and enforce engineering standards – linked to SC1, SC2, SC5

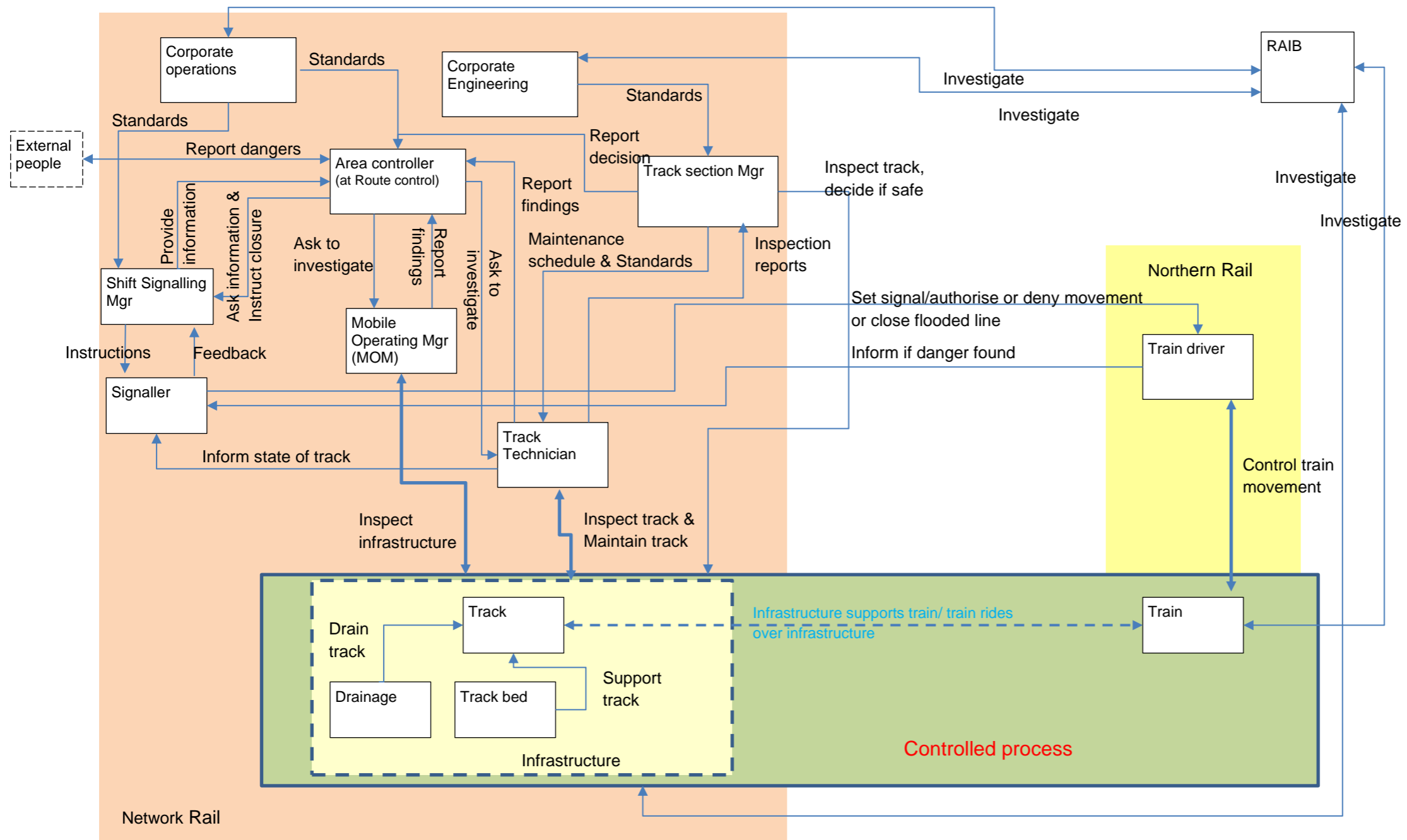


Figure 54 Developed control structure

H3.3 Stage 3 - Identify unsafe control actions (UCAs)

Table 111 Signaller unsafe control actions

Component	Signaller			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Set signal /set route	N/a	UC1: Signal set to green when line damaged - linked to H2	N/a	N/a
Authorise movement	N/a	UCA2: Movement authorised when line damaged - linked to H2	N/a	N/a
Deny movement authority	UCA3: Denial of movement authority and blocking of the line not carried out when flood/damage is reported – linked to H2, H1	N/a	UCA4: Denial of movement authority and blocking of the line not carried out quickly enough when flood/damage is reported and train is beyond signal – linked to H2, H1	UCA5: Denial of movement authority and blocking of the line removed before flood/damage is corrected – linked to H2, H1
Close flooded line	UCA6: Flooded line open to traffic – linked to H1	UCA7: Wrong line closed while flooded line remains open – linked to H2	UCA8: Line not closed quickly enough and train is beyond signal – linked to H1	UCA9: Line reopened while still flooded – linked to H1

Note that in the current context of a damaged line the denial of a movement authority is not unsafe.

Table 112 Signalling manager unsafe control actions

Component	Signalling Mgr			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Instruct signaller	UCA10: Instruction to block a damaged line not provided – linked to H2	UCA11: Instruct the signaller to set route when the line is damaged – linked to H2	UCA12: Instruction to block a line is provided after a train has passed the controlling signal – linked to H2	UCA13: Instruction to block a damaged line is rescinded before it is fixed – linked to H2

Table 113 Mobile Operations Manager unsafe control actions

Component	Mobile Operations Mgr			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Inspect infrastructure	UCA14: The inspection has not taken place – linked to H2, H1	UCA15: The wrong infrastructure is inspected – linked to H2	UCA16: The inspection is not undertaken when required – linked to H2, H1	UCA17: Inspection stopped before damaged section identified – linked to H1, H2

The inspection either takes place or not there is no length issue. The length of an inspection is related to a geospatial length.

Table 114 Track Technician unsafe control actions

Component	Track technician			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Inspect track	UCA18: The track inspection has not taken place and the track is in an	UCA19: The wrong track is inspected – linked to H2	UCA20: The track inspection is not undertaken	UCA21: Inspection stopped before damaged section

	unknown condition – linked to H2, H1		when required – linked to H2	identified – linked to H1, H2
Report inspection findings	UCA57: The report of the inspection is not provided – linked to H2	UCA58: The report of the inspection is not correct – linked to H2	UCA59: The report is delivered after it is required – linked to H2	N/a
Maintain track	UCA22: Track maintenance has not taken place -linked to H1	UCA23: Track not maintained to standards – linked to H1	UCA24: Periodicity not met – linked to H2	N/a

Table 115 Track Section Manager unsafe control actions

Component	Track section manager			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Maintenance schedule	UCA25: Track is unmaintained -linked to H1, H2	UCA26: The schedule allows track to become dangerous – linked to H1, H2	UCA27: Maintenance is scheduled in the wrong order – linked to H1, H2	N/a
Instruct and enforce standards	UCA28: Standards not implemented -linked to H1	UCA29: Track maintained to wrong limits – linked to H1	UCA30: Old standards are used -linked to H1	N/a
Inspect track, decide if safe	UCA31: Track is in an unknown state – linked to H2	UCA32: Damaged track is declared safe – linked to H2	N/a	UCA33: Inspection stopped before damaged section identified – linked to H2, H1
Report decision	UCA34: Damaged line left open to traffic – linked to H2	N/a	UCA35: Damaged line left open to traffic – linked to H2	N/a

Table 116 Area Controller unsafe control actions

Component	Area Controller			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Ask information	UCA36: Information about trains not requested when line damaged – linked to H2	UCA37: Information requested about the wrong area – linked to H2	UCA38: Information requested after long delay allowing trains to continue in meantime – linked to H2	N/a
Instruct closure	UCA39: Closure of damaged line is not ordered – linked to H2	UCA40: Closure of wrong line instructed – linked to H2	UCA41: Closure instructed after long delay allowing trains to continue in meantime – linked to H2	UCA42: Line opened to traffic while still damaged – H2
Ask to investigate	UCA43: Request to investigate damage report not given and damaged line remains open – linked to H2	UCA44: Request to investigate the wrong area – linked to H2	UCA45: Request to investigate a report given after long delay while trains continue to operate – linked to H2	UCA46: Request for investigation stopped before damage found – linked to H2

Table 117 Corporate Operations unsafe control actions

Component	Corporate operations			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Set/issue standards	UCA47: Current standards not provided and old standards continue to be	UCA48: Incorrect standard issued and line operated to wrong parameters –	UCA49: Tasks are set out incorrectly allowing dangerous condition – linked to H2	N/a

	used – H2, H1	linked to H1, H2		
--	------------------	---------------------	--	--

Table 118 Corporate Engineering unsafe control actions

Component	Corporate Engineering			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Set/issue standards	UCA50: Current standards not provided and old standards continue to be used – linked to H1	UCA51: Incorrect standard issued and line maintained to wrong parameters – linked to H1	UCA52: Tasks are set out incorrectly leaving line still in dangerous condition – linked to H1	N/a

Table 119 Driver unsafe control actions

Component	Driver			
Control action	Not provided	Wrong action	Not on time or out of sequence	Stopped too soon or late
Control train	UCA53: Train is out of control – linked to H3	UCA54: Train is driven over closed line – linked to H3	UCA55: Braking too late and running over damaged line – linked to H1	UCA56: Braking stopped too soon and train rolls over damaged line – linked to H1

Controller constraints

Table 120 Controller constraints to prevent unsafe control actions

Controller	Unsafe control actions	Controller constraints
Signaller		
	UC1: Signal set to green when line damaged -linked to H2	C1: Signal must be set to red when line damaged – linked to UCA1
	UCA2: Movement authorised when line damaged -linked to H2	C2: Movement must not be authorised when the line is damaged – linked to UCA2
	UCA3: Denial of movement authority and blocking of the line not carried out when flood/damage is reported – linked to H2, H1	C3: Movement must not be authorised when the line is flooded or damaged – linked to UCA3, UCA5, UCA6, UCA9
	UCA4: Denial of movement authority and blocking of the line not carried out quickly enough when flood/damage is reported and train is beyond signal – linked to H2, H1	C4: The line must be blocked immediately when flooding or damage is reported – linked to UCA4, UCA8
	UCA5: Denial of movement authority and blocking of the line removed before flood/damage is corrected – linked to H2, H1	C3: Movement must not be authorised when the line is flooded or damaged – linked to UCA5, UCA3, UCA6, UCA9

Controller	Unsafe control actions	Controller constraints
	UCA6: Flooded line open to traffic – linked to H1	C3: Movement must not be authorised when the line is flooded or damaged – linked to UCA5, UCA3, UCA6
	UCA7: Wrong line closed while flooded line remains open – linked to H2	C7: The correct line must be closed when flooding is reported – linked to UCA7
	UCA8: Line not closed quickly enough and train is beyond signal – linked to H1	C4: The line must be blocked immediately when flooding or damage is reported – linked to UCA4, UCA8
	UCA9: Line reopened while still flooded – linked to H1	C3: Movement must not be authorised when the line is flooded or damaged – linked to UCA5, UCA3, UCA6, UCA9
Signalling Mgr		
	UCA10: Instruction to block a damaged line not provided – linked to H2	C10: Instruction to block a damaged line must be given – linked to UCA10
	UCA11: Instruct the signaller to set route when the line is damaged – linked to H2	C11: The signaller must not be instructed to set route when the line is damaged – linked to UCA11
	UCA12: Instruction to block a line is provided after a train has passed the controlling signal – linked to H2	C12: Instruction to block a line must be provided immediately – linked to UCA12

Controller	Unsafe control actions	Controller constraints
	UCA13: Instruction to block a damaged line is rescinded before it is fixed – linked to H2	C13: Instruction to open the line must not be given before it is fixed – linked to UCA13
Mobile Operations Mgr		
	UCA14: The inspection has not taken place – linked to H2, H1	C14: The inspection must take place when requested – linked to UCA14, UCA16
	UCA15: The wrong infrastructure is inspected – linked to H2	C15: The correct infrastructure must be inspected – linked to UCA15
	UCA16: The inspection is not undertaken when required – linked to H2, H1	C14: The inspection must take place when requested – linked to UCA14, UCA16
Track Technician		
	UCA17: Inspection stopped before damaged section identified – linked to H1, H2	C17: The damaged section must be identified – linked to UCA17, UCA21
	UCA18: The track inspection has not taken place and the track is in an unknown condition – linked to H2, H1	C18: Track inspections must take place when required – linked to UCA18, UCA20
	UCA19: The wrong track is inspected – linked to H2	C19: The correct track must be inspected – linked to UCA19

Controller	Unsafe control actions	Controller constraints
	UCA20: The track is not undertaken when required – linked to H2	C18: Track inspections must take place when required – linked to UCA18, UCA20
	UCA21: Inspection stopped before damaged section identified – linked to H1, H2	C17: The damaged section must be identified – linked to UCA17, UCA21
	UCA57: The report of the inspection is not provided – linked to H2	C57: The report of the inspection must be delivered – linked to UCA57
	UCA58: The report of the inspection is not correct – linked to H2	C58: The report of the inspection must be accurate – linked to UCA58
	UCA59: The report is delivered after it is required – linked to H2	C59: The report must be delivered when it is needed and of use – linked to UCA59
	UCA22: Track maintenance has not taken place -linked to H1	C22: Track maintenance must take place when required – linked to UCA22, UCA24
	UCA23: Track not maintained to standards – linked to H1	C23: Track must be maintained to standards – linked to UCA23
	UCA24: Periodicity not met – linked to H2	C22: Track maintenance must take place when required – linked to UCA22, UCA24
Track Section Mgr		
	UCA25: Track is unmaintained -linked to H1, H2	C25: Track must be maintained – linked to UCA25

Controller	Unsafe control actions	Controller constraints
	UCA26: The schedule allows track to become dangerous – linked to H1, H2	C26: The track must be maintained to a safe schedule – linked to UCA26
	UCA27: Maintenance is scheduled in the wrong order – linked to H1, H2	C27: The maintenance must be scheduled in the right order – linked to UCA27
	UCA28: Standards not implemented -linked to H1	C28: Standards must be implemented – linked to UCA28
	UCA29: Track maintained to wrong limits – linked to H1	C29: Track must be maintained to the correct limits – linked to UCA29
	UCA30: Old standards are used -linked to H1	C30: Current standards must be used – linked to UCA30
	UCA31: Track is in an unknown state – linked to H2	C31: Track status must be obtained – linked to UCA31
	UCA32: Damaged track is declared safe – linked to H2	C32: Track must only be declared safe when it is within standards – linked to UCA32
	UCA33: Inspection stopped before damaged section identified – linked to H2, H1	C33: Inspection must identify the damaged section – linked to UCA33
	UCA34: Damaged line left open to traffic – linked to H2	C34: Damaged line must be closed – linked to UCA34, UCA35

Controller	Unsafe control actions	Controller constraints
	UCA35: Damaged line left open to traffic – linked to H2	C34: Damaged line must be closed – linked to UCA34, UCA35
Area Controller		
	UCA36: Information about trains not requested when line damaged – linked to H2	C36: Information about train positions must be requested when the line is damaged – linked to UCA36
	UCA37: Information requested about the wrong area – linked to H2	C37: Information must be requested about the correct area – linked to UCA37
	UCA38: Information requested after long delay allowing trains to continue in meantime – linked to H2	C38: Information must be requested immediately – linked to UCA38
	UCA39: Closure of damaged line is not ordered – linked to H2	C39: Closure of the damaged line must be ordered – linked to UCA39
	UCA40: Closure of wrong line instructed – linked to H2	C40: The correct line must be closed – linked to UCA40
	UCA41: Closure instructed after long delay allowing trains to continue in meantime – linked to H2	C41: The line must be closed immediately when damaged – linked to UCA41, UCA42
	UCA42: Line opened to traffic while still damaged – H2	C41: The line must be closed immediately when damaged – linked to UCA41, UCA42

Controller	Unsafe control actions	Controller constraints
	UCA43: Request to investigate damage report not given and damaged line remains open – linked to H2	C43: Request to investigate reported damage to line must be given – linked to UCA43
	UCA44: Request to investigate the wrong area – linked to H2	C44: The request to investigate damage must be given for the right area – linked to UCA44
	UCA45: Request to investigate a report given after long delay while trains continue to operate – linked to H2	C43: Request to investigate reported damage to line must be given immediately – linked to UCA45
	UCA46: Request for investigation stopped before damage found – linked to H2	C44: Request for investigation into damage must continue until damage found – linked to UCA46
Corporate operations		
	UCA47: Current standards not provided and old standards continue to be used – H2, H1	C47: Current operational standards must be provided – linked to UCA47
	UCA48: Incorrect standard issued and line operated to wrong parameters – linked to H1, H2	C48: The correct operating standard must be issued – linked to UCA48
	UCA49: Tasks are set out incorrectly allowing dangerous condition – H2	C49: Operational tasks must be set out correctly – linked to UCA49

Controller	Unsafe control actions	Controller constraints
Corporate engineering		
	UCA50: Current standards not provided and old standards continue to be used – H1	C50: Current engineering standards must be provided – linked to UCA50
	UCA51: Incorrect standard issued and line maintained to wrong parameters – linked to H1	C51: The correct engineering standard must be issued – linked to UCA51
	UCA52: Tasks are set out incorrectly leaving line still in dangerous condition – H1	C52: Engineering tasks must be set out correctly – linked to UCA52
Driver		
	UCA53: Train is out of control – linked to H3	C53: The train driver must be in control of the train at all times – linked to UCA53
	UCA54: Train is driven over closed line – linked to H3	C54: Train must not be driven over a closed line – linked to UCA54
	UCA55: Braking too late and running over damaged line – linked to H1	C55: Train must be braked early enough to stop before damaged section of line – linked to UCA55
	UCA56: Braking stopped too soon and train rolls over damaged line – H1	C56: Braking must be applied until the train comes to a stop – linked to UCA56

H3.4 Stage 4 - Identify loss scenarios

The actuators and sensors are inserted into the control structure to aid scenario identification.

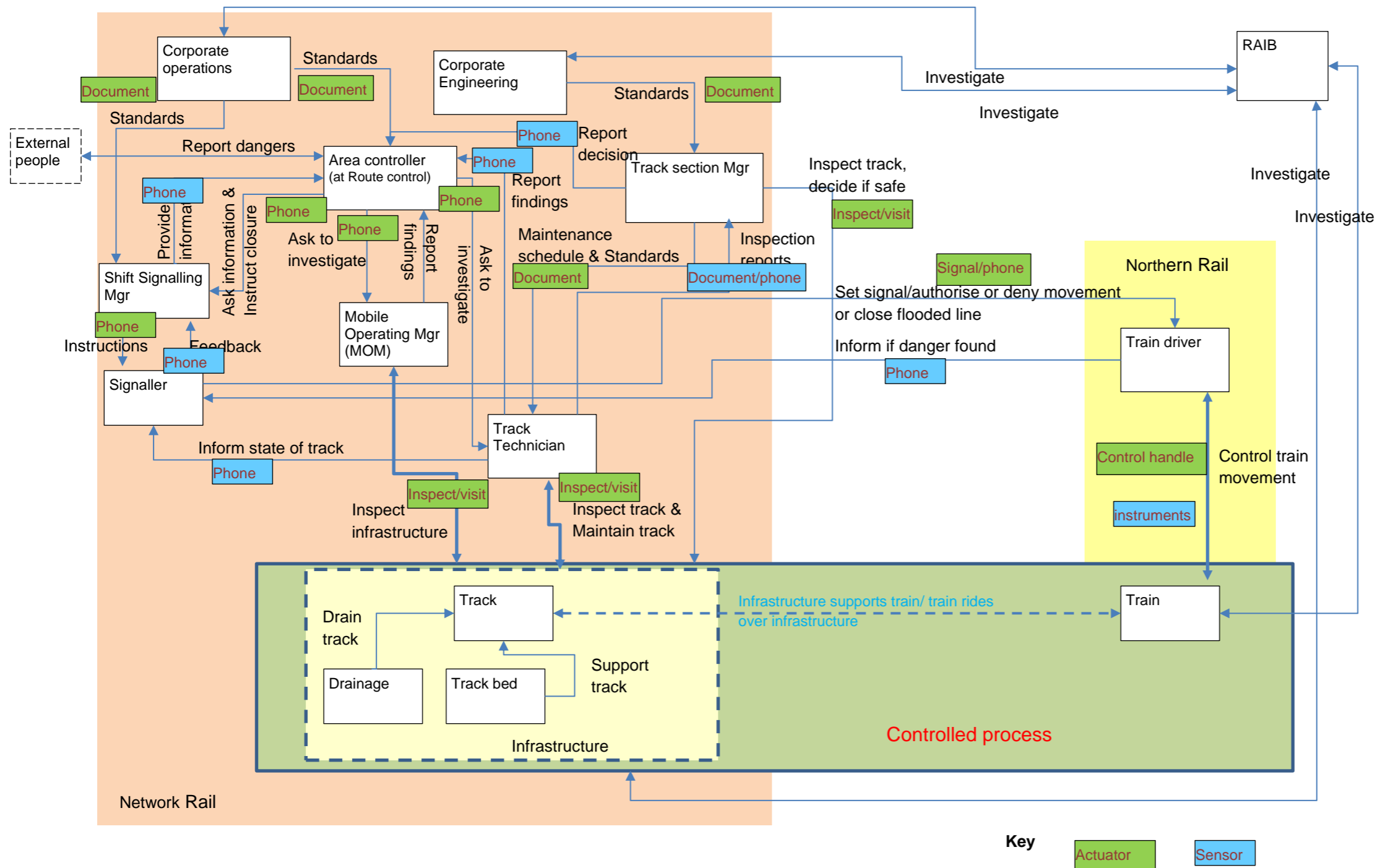


Figure 55 Developed control structure with actuators and sensors overlaid

Unsafe controller action scenarios

Table 121 Scenario analysis for unsafe controller actions

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
Signaller									
	UC1: Signal set to green when line damaged -linked to H2								
			✓		Sen1 for UCA1: Signal set to green by signaller when the line is damaged because he is unaware of the damage – linked to H2	unaware of the damage	20		
		✓			Sen2 for UCA1: Signal set to green by signaller when the line is damaged because he considers damage minor – linked to H2	misjudgement			✓
				✓	Sen3 for UCA1: Signal set to green by signaller when the line is damaged because he has not been phoned or told about the damage – linked to H2	No communication	22		
	UCA2: Movement authorised when line damaged -linked to H2								

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
			✓		Sen1 for UCA2: Movement authorised by signaller when the line is damaged because he is unaware of the damage – linked to H2	unaware of the damage	20		
		✓			Sen2 for UCA2: Movement authorised by signaller when the line is damaged because he considers damage minor – linked to H2	misjudgement			✓
				✓	Sen3 for UCA2: Signal set to green by signaller when the line is damaged because he has not been phoned or told about the damage – linked to H2	No communication	22		
	UCA3: Denial of movement authority and blocking of the line not carried out when flood/damage is reported – linked to H2, H1								
		✓			Sen1 for UCA3: Movement authorities still issued for a period allowing trains to travel on damaged line while veracity of damage checked – linked to H2, H1	Uncertainty			✓
		✓			Sen2 for UCA3: Movement authorities still issued for a period while management support is sought allowing trains to travel on the damaged line – linked to H2, H1	Lack of authority			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	UCA4: Denial of movement authority and blocking of the line not carried out quickly enough when flood/damage is reported and train is beyond signal – linked to H2, H1								
		✓			Sen1 for UCA4: Movement authorities still issued for a period allowing trains to travel on damaged line while veracity of damage checked – linked to H2, H1	Uncertainty			✓
		✓			Sen2 for UCA4: Movement authorities still issued for a period while management support is sought allowing trains to travel on the damaged line – linked to H2, H1	Lack of authority			✓
	UCA5: Denial of movement authority and blocking of the line removed before flood/damage is corrected – linked to H2, H1								
		✓			Sen1 for UCA5: Movement authority is restored due to signaller misunderstanding	Misjudgement	19, 20		

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					the status of the line leading to trains operating on the damaged line – linked to H2, H1				
	UCA6: Flooded line open to traffic – linked to H1								
		✓			Sen1 for UCA6: Flooded line open to traffic because the signaller does not think it meets the requirements of the rule book for closure (above the rails) leading to trains travelling on a damaged line – linked to H1	Misjudgement			✓
			✓		Sen2 for UCA6: Flooded lined not reported to the signaller and the signaller is unaware. Consequently, the line is open and trains are travelling on the damaged line – linked to H1	No communication			✓
	UCA7: Wrong line closed while flooded line remains open – linked to H2								
		✓			Sen1 for UCA7: The signaller misunderstands where the line is flooded and closes the wrong line. Consequently, trains continue to travel over the damaged/flooded line – linked to H2	misinterpretation			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
				✓	Sen2 for UCA7: The signaller does not hear the phone message properly where the line is flooded and closes the wrong line. Consequently, trains continue to travel over the damaged/flooded line – linked to H2	Miscommunication			✓
	UCA8: Line not closed quickly enough and train is beyond signal – linked to H1								
		✓			Sen1 for UCA8: The damaged line is not closed quickly enough because the signaller is dealing with other signalling issues and trains continue to be routed over the damaged line – linked to H1	Busy			✓
		✓			Sen2 for UCA8: Movement authorities still issued for a period allowing the train to travel beyond the signal on damaged line while veracity of damage checked – linked to H1	Uncertainty			✓
		✓			Sen3 for UCA8: Movement authorities still issued for a period while management support is sought allowing train to travel beyond the signal to travel on the damaged line – linked to H1	Lack of authority			✓
				✓	Sen4 for UCA8: Movement authorities still issued for a period because there is a delay	Slow communication	5		

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					in phoning the signaller allowing train to travel beyond the signal to travel on the damaged line – linked to H1				
	UCA9: Line reopened while still flooded – linked to H1								
			✓		Sen1 for UCA9: The line is reopened because the signaller is given the impression that it is not now flooded. Consequently, trains are allowed to travel on the flooded line – linked to H1	Incorrect information	19, 20		
				✓	Sen2 for UCA9: The line is reopened because the signaller mishears the phone message and thinks that it is not now flooded. Consequently, trains are allowed to travel on the flooded line – linked to H1	Miscommunication			✓
Signalling Mgr									
	UCA10: Instruction to block a damaged line not provided – linked to H2								
		✓			Sen1 for UCA10: An instruction to block a damaged line is not given because the signalling manager is distracted. As a result,	Distraction			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					trains continue to be routed over the line – linked to H2				
		✓			Sen2 for UCA10: An instruction to block a damaged line is not given because the signalling manager does not consider the damage warrants it. As a result, trains continue to travel over the damaged line – lined to H2	Misjudgement			✓
				✓	Sen3 for UCA10: An instruction to block a damaged line is not given because the signalling manager does not receive a phone call about it. As a result, trains continue to travel over the damaged line – lined to H2	No communication	22		
	UCA11: Instruct the signaller to set route when the line is damaged – linked to H2								
		✓			Sen1 for UCA11: The signalling manager instructs the signaller to continue to set routes over the damaged line because he believes it is not badly damaged. As a result, trains are routed over the damaged line – linked to UCA11	Misjudgement			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
		✓			Sen2 for UCA11: The signalling manager instructs the signaller to continue to set routes over the damaged line to keep the timetable running. As a result, trains are routed over the damaged infrastructure – linked to H2	Misjudgement			✓
	UCA12: Instruction to block a line is provided after a train has passed the controlling signal – linked to H2								
		✓			Sen1 for UCA12: The signalling manager gives an instruction to block a damaged line after a train has passed the controlling signal because he is distracted by other tasks which delays the action. Consequently, a train is routed along a damaged line – linked to H2	Busy			✓
	UCA13: Instruction to block a damaged line is rescinded before it is fixed – linked to H2								
			✓		Sen1 for UCA13: The signalling manager instructs the signaller to resume routing trains on the damaged line before it is fix	Incorrect information			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					because he believes it has been fixed – linked to H2				
Mobile Operations Mgr									
	UCA14: The inspection has not taken place – linked to H2, H1								
		✓			Sen1 for UCA14: The line is not inspected because the MOM is not able to get onto the line to inspect it. As a result, the line's status remains unknown – linked to H2, H1	Inability to act	3		
	UCA15: The wrong infrastructure is inspected – linked to H2								
		✓			Sen1 for UCA15: The wrong line is inspected because the MOM does not go to the right location. As a result, the line's status remains unknown – linked to H2	Lack of knowledge	17, 18		
				✓	Sen2 for UCA15: The wrong line is inspected because the MOM does not hear the location correctly due to noise. As a result, the line's status remains unknown – linked to H2	Miscommunication			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	UCA16: The inspection is not undertaken when required – linked to H2, H1								
				✓	Sen1 for UCA16: The inspection is not undertaken when required because there is a delay in getting to the location. As a result, the line's status remains unknown – linked to H1, H2	Operative not local			✓
Track Technician									
	UCA17: Inspection stopped before damaged section identified – linked to H1, H2								
		✓			Sen1 for UCA17: The inspection is stopped before the damaged section is identified because the location of the damaged section is unknown and the technician judges nothing is wrong as a long section has been inspected. As a result, the line's status remains unknown – linked to H1, H2	Lack of knowledge	17, 20		
		✓			Sen2 for UCA17: The inspection is stopped before the damaged section is identified because the available time for the task has	Lack of time			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					expired. As a result, the line's status remains unknown – linked to H1, H2				
	UCA18: The track inspection has not taken place and the track is in an unknown condition – linked to H2, H1								
				✓	Sen1 for UCA18: The track inspection has not taken place because the request has not reached the track technician. Consequently, the condition of the line remains unknown – linked to H1, H2	No communication			✓
		✓			Sen2 for UCA18: The track inspection has not taken place because the track technician has more important tasks to complete first. Consequently, the condition of the line remains unknown – linked to H1, H2	Busy			✓
	UCA19: The wrong track is inspected – linked to H2								
			✓		Sen1 for UCA19: The wrong track is inspected because the wrong location is given to the track technician. Consequently,	Misinformation	17		

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					the condition of the line remains unknown – linked to H2				
				✓	Sen2 for UCA19: The wrong track is inspected because the track technician did not hear the location properly. Consequently, the condition of the line remains unknown – linked to H2	Miscommunication			✓
	UCA20: The track is not undertaken when required – linked to H2								
		✓			Sen1 for UCA20: The track is not inspected when required because the track technician is busy with other tasks (such as maintenance).	Busy			✓
				✓	Sen2 for UCA20: The track is not inspected when required because the track technician is in another location.	Operative not local			✓
	UCA21: Inspection stopped before damaged section identified – linked to H1, H2								
		✓			Sen1 for UCA21: The track inspection is stopped before the damaged section is found because the allotted time has	Lack of time			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					expired. As a result, the damaged line is opened to traffic – linked to H1, H2				
	UCA57: The report of the inspection is not provided – linked to H2								
			✓		Sen1 for UCA57: The track inspection has taken place but a report of the findings is not provided to the requester. As a result, no information is fed back – linked to H2	No report			✓
	UCA58: The report of the inspection is not correct – linked to H2								
			✓		Sen1 for UCA58: The report of the findings is incorrect. As a result, the person relying of the report takes the wrong action – linked to H2	Misinformation	20		
	UCA59: The report is delivered after it is required – linked to H2								
			✓		Sen1 for UCA59: The report is delivered late and events have occurred in the meantime. As a result, trains have run over damaged track – linked to H2	Late information			✓
	UCA22: Track maintenance has not								

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	taken place -linked to H1								
		✓			Sen1 for UCA22: The track maintenance has not taken place due to a lack of resources. As a result, a substandard line is open to traffic which could collapse – linked to H1	Lack of resources			✓
	UCA23: Track not maintained to standards – linked to H1								
			✓		Sen1 for UCA23: The track is not maintained to standards because the maintenance technician has not been briefed. As a result, substandard track is open to traffic which could collapse – linked to H1	No communication			✓
	UCA24: Periodicity not met – linked to H2								
		✓			Sen1 for UCA24: The track is not maintained and inspected to the frequency required because of a lack of resources. As a result, the track could have deteriorated and collapse under a train – linked to H2	Lack of resources			✓
Track Section Mgr									

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	UCA25: Track is unmaintained -linked to H1, H2								
		✓			Sen1 for UCA25: The track is unmaintained because a schedule has not been created for its maintenance. As a result, damaged track which could lead to a derailment – linked to H2	Task not done			✓
		✓			Sen2 for UCA25: the track is not maintained because the necessary resources are not available. As a result, damaged track which could lead to a derailment – linked to H2	Lack of resources			✓
	UCA26: The schedule allows track to become dangerous – linked to H1, H2								
		✓			Sen1 for UCA26: The schedule is not frequent enough allowing to track to become dangerous because there is a lack of resources available to do anything more frequent. As a result, damaged track which could lead to a derailment – linked to H1, H2	Misjudgement			✓
	UCA27: Maintenance is scheduled in the								

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	wrong order – linked to H1, H2								
			✓		Sen1 for UCA27: The Maintenance tasks are scheduled in the wrong order because the standards are confused. As a result, later tasks undo the work of earlier tasks resulting in substandard track which could derail a train – linked to H1, H2	Misinformation			✓
	UCA28: Standards not implemented -linked to H1								
			✓		Sen1 for UCA28: The standards are not implemented in the maintenance of track because the section manager is unaware of their existence. As a result, the line could deteriorate resulting in a derailment – linked to H1	No communication			✓
	UCA29: Track maintained to wrong limits – linked to H1								
			✓		Sen1 for UCA29: The track is maintained to the wrong limits because the section manager is unaware of the current limits. As a result, the line could deteriorate resulting in a derailment – linked to H1	No communication			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	UCA30: Old standards are used -linked to H1								
			✓		Sen1 for UCA29: The track is maintained to old standards because the section manager is unaware of the current limits. As a result, the line could deteriorate resulting in a derailment – linked to H1	No communication			✓
	UCA31: Track is in an unknown state – linked to H2								
		✓			Sen1 for UCA31: The track is in an unknown state because it has not been inspected. As a result, the line could deteriorate resulting in a derailment – linked to H2	Task not done			✓
	UCA32: Damaged track is declared safe – linked to H2								
		✓			Sen1 for UCA32: Damaged track is declared safe because the damage has not been identified. As a result, the line could deteriorate resulting in a derailment – linked to H2	Misjudgement			✓
		✓			Sen2 for UCA32: Damaged track is declared safe because the section manager does not appreciate the significance of the	Misjudgement			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					damage. As a result, the line could deteriorate resulting in a derailment – linked to H2				
	UCA33: Inspection stopped before damaged section identified – linked to H2, H1								
		✓			Sen1 for UCA33: Inspection stopped before damaged section identified because the time allowed has expired. As a result, the line could be in a substandard state resulting in a derailment – linked to H1, H2	Lack of time			✓
		✓			Sen2 for UCA33: Inspection stopped before damaged section identified because the damage was missed. As a result, the line could be in a substandard state resulting in a derailment – linked to H1, H2	Missed identification			✓
	UCA34: Damaged line left open to traffic – linked to H2								
		✓			Sen1 for UCA34: The damaged line is left open to traffic because the damage is not considered serious. As a result, the line could be in a substandard state resulting in a derailment – linked to H2	Misjudgement			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	UCA35: Damaged line left open to traffic – linked to H2								
		✓			Sen1 for UCA35: The damaged line is left open to traffic because the decision to leave the line open was taken out of sequence and does not take account of inspection reports. As a result, the line could be in a substandard state resulting in a derailment – linked to H2	Misjudgement			✓
Area Controller									
	UCA36: Information about trains not requested when line damaged – linked to H2								
		✓			Sen1 for UCA36: Information about the trains whereabouts is not requested when the line is damaged because the controller is attending to other duties. As a result, the line is left open to traffic which could result in a derailment – linked to H2	Busy			✓
		✓			Sen2 for UCA36: Information about the trains whereabouts is not requested when the line is damaged because the controller	Distracted			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					forgets to ask. As a result, the line is left open to traffic which could result in a derailment – linked to H2				
	UCA37: Information requested about the wrong area – linked to H2								
		✓			Sen1 for UCA37: Information is requested about the wrong area because the controller mistakes the location of the problem. As a result, the line is left open to traffic which could result in a derailment – linked to H2	Lack of knowledge			✓
				✓	Sen2 for UCA37: Information is requested about the wrong area because the controller's phone message is not received clearly. As a result, the line is left open to traffic which could result in a derailment – linked to H2	Miscommunication	17		
	UCA38: Information requested after long delay allowing trains to continue in meantime – linked to H2								
		✓			Sen1 for UCA38: Information is requested after a long delay because it takes time to verify the parameters of the request. As a	Uncertainty			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					result, trains continue to operate on a damaged line that could result in a derailment – linked to H2				
		✓			Sen1 for UCA38: Information is requested after a long delay because the controller is busy attending to other duties. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Busy			✓
	UCA39: Closure of damaged line is not ordered – linked to H2								
		✓			Sen1 for UCA39: The closure of damaged line is not ordered because it is thought that the damage is slight. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Misjudgement	16		
		✓			Sen2 for UCA39: The closure of damaged line is not ordered because of a requirement to keep the timetable operational. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Misjudgement			✓
			✓		Sen3 for UCA39: The closure of damaged line is not ordered because information is not received via the phone. As a result,	No communication			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					trains continue to operate on a damaged line that could result in a derailment – linked to H2				
	UCA40: Closure of wrong line instructed – linked to H2								
		✓			Sen1for UCA40: Closure of the wrong line is instructed because there is confusion over the location of the damage. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Lack of knowledge	17		
				✓	Sen1for UCA40: Closure of the wrong line is instructed because there is confusion over the location because the phone call is misheard. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Miscommunication			✓
	UCA41: Closure instructed after long delay allowing trains to continue in meantime – linked to H2								
		✓			Sen1 for UCA41: closure of the line is instructed after a long delay because the controller is busy attending to other duties.	Busy			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2				
		✓			Sen2 for UCA41: closure of the line is instructed after a long delay because the there is a delay is the controller obtaining management support to act. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Lack of authority			✓
	UCA42: Line opened to traffic while still damaged – H2								
			✓		Sen1 for UCA42: The line is opened to traffic by the controller due to misinformation about the status of the line. As a result, trains begin to operate on a damaged line that could result in a derailment – linked to H2	Misinformation			✓
	UCA43: Request to investigate damage report not given and damaged line remains open – linked to H2								
		✓			Sen1 for UCA43: A request to investigate a damage report received externally is not	Distraction	5, 16, 22		

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					given because the controller is distracted and forgets. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2				
	UCA44: Request to investigate the wrong area – linked to H2								
			✓		Sen1 for UCA44: The request to investigate is for the wrong area due to confusion over the location of the reported damage. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	misinformation	17		
				✓	Sen2 for UCA44: The request to investigate is for the wrong area due to confusion over the location caused by mishearing the phone call of the reported damage. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Miscommunication			✓
	UCA45: Request to investigate a report given after long delay while trains continue to operate – linked to H2								

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
		✓			Sen1 for UCA45: A request to investigate a report is delayed for a long period because the controller is busy attending to other duties. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Busy			✓
	UCA46: Request for investigation stopped before damage found – linked to H2								
		✓			Sen1 for UCA46: The request for an investigation is stopped before the damage is found by the controller because of pressure to restore operations. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Management pressure			✓
Corporate operations									
	UCA47: Current standards not provided and old standards continue to be used – H2, H1								
		✓			Sen1 for UCA47: Current standards are not issued through the corporate standards	Administration error			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
					process due to an administration error. As a result, trains continue to operate on a potentially damaged line that could result in a derailment – linked to H1, H2				
	UCA48: Incorrect standard issued and line operated to wrong parameters – linked to H1, H2								
		✓			Sen1 for UCA48: An incorrect standard is issued with wrong parameters because of a mistake is the drafting. As a result, trains continue to operate on a potentially damaged line that could result in a derailment – linked to H1, H2	Drafting error			✓
	UCA49: Tasks are set out incorrectly allowing dangerous condition – H2								
		✓			Sen1 for UCA49: Tasks are set out incorrectly allowing a dangerous condition because of a standards' drafting error. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H2	Drafting error			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
Corporate engineering									
	UCA50: Current standards not provided and old standards continue to be used – H1								
		✓			Sen1 for UCA50: Current standards are not issued through the corporate standards process due to an administration error. As a result, trains continue to operate on a potentially damaged line that could result in a derailment – linked to H1	Administrative error			✓
	UCA51: Incorrect standard issued and line maintained to wrong parameters – linked to H1								
		✓			Sen1 for UCA51: An incorrect standard is issued with wrong engineering parameters because of a mistake in the drafting. As a result, trains continue to operate on a potentially damaged line that could result in a derailment – linked to H1	Drafting error			✓
	UCA52: Tasks are set out incorrectly leaving								

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	line still in dangerous condition – H1								
		✓			Sen1 for UCA52: Tasks are set out incorrectly allowing a dangerous condition because of a standards' drafting error. As a result, trains continue to operate on a damaged line that could result in a derailment – linked to H1	Drafting error			✓
Driver									
	UCA53: Train is out of control – linked to H3								
		✓			Sen1 for UCA53: The train is out of control because the driver has made a mistake and over accelerated. As a result, the train cannot stop in time resulting in a potential derailment – linked to H3	Misjudgement			✓
	UCA54: Train is driven over closed line – linked to H3								
		✓			Sen1 for UCA54: The train is driven over a closed line because the driver did not recognise the red signal. As a result, the train is operating over a damaged line which could result in a derailment – linked to UCA54	Missed communication			✓

Controller	Unsafe control actions	Scenario type			Scenarios	Causes	Source verification		
		Unsafe controller behaviour	Inadequate feedback & information	Control path			Source incident facts	Source context facts	No facts found
	UCA55: Braking too late and running over damaged line – linked to H1								
		✓			Sen1 for UCA55: Braking has been left too late because the driver has misjudged the braking point. As a result, the train is operating over a damaged line which could result in a derailment – linked to UCA55	Misjudgement	10		
	UCA56: Braking stopped too soon and train rolls over damaged line – H1								
		✓			Sen1 for UCA56: Braking has stopped too soon and the train rolls over the damaged line because the braking has been misjudged. As a result, the train is operating over damaged infrastructure which could result in the train becoming unstable and a derailment – linked to UCA56	Misjudgement			✓

Scenarios for controllers without Unsafe Control Actions

Table 122 Scenario analysis of controller actions

Controller	Control actions	Scenario type		Scenarios	Causes	Source verification		
		Control action not implemented	Control action improperly implemented			Source incident facts	Source context facts	No facts found
Signaller								
	Set signal /set route			Not unsafe				
	Authorise movement			Not unsafe				
	Deny movement authority							
		✓		Sen1: The movement authority is not denied to a train when the line is damaged. As a result, the train operates over damaged infrastructure leading to a possible derailment – linked to H1	Movement authority given	9, 20		
		✓		Sen2: The movement authority via the signalling and the route is left set for a train when the line is damaged. As a result, the train operates over damaged infrastructure leading to a possible derailment – linked to H1	Route is not cancelled			✓
			✓	Sen3: Signaller does not contact all trains to withdraw a previously given movement authority	No Communication			✓
	Close flooded line							
		✓		Sen1: The movement authority via the signalling and the route is left set for a train when the line is damaged. As a result, the train	Route is not cancelled	9		

Controller	Control actions	Scenario type		Scenarios	Causes	Source verification		
		Control action not implemented	Control action improperly implemented			Source incident facts	Source context facts	No facts found
				operates over damaged infrastructure leading to a possible derailment – linked to H1				
			✓	Sen2: The line is not closed as per the rules and another signaller could route trains – linked to H1	Did not follow rules			✓
Signalling Mgr								
	Instruct signaller							
		✓		Sen1: Signalling Manager does not instruct the signaller because of difficulty in contacting the signaller. As a result, the line is left open to traffic and a potential derailment – linked to H2	Difficult communication			✓
Mobile Operations Mgr								
	Inspect infrastructure							
		✓		Sen1: MOM does not inspect infrastructure because he does not have the authority to access the line – linked to H2	No authority	3		
		✓		Sen2: MOM does not inspect infrastructure because he medically fit to be on the line – linked to H2	Medically unfit	3		
Track Technician								
	Inspect track							

Controller	Control actions	Scenario type		Scenarios	Causes	Source verification		
		Control action not implemented	Control action improperly implemented			Source incident facts	Source context facts	No facts found
		✓		Sen1: The Track Technician does not inspect the track because he is unavailable – linked to H1	Not available			✓
			✓	Sen2: The Track Technician does not inspect the track properly due to time limitations and just carries out a cursory look. As a result, the damage is undetected leading to a possible derailment – linked to H1	Lack of time			✓
	Report findings							
				Sen1: The Track Technician does not report findings accurately. As a result, a misimpression is given – linked to H2	Not accurate			✓
	Maintain track							
			✓	Sen1: The Track Technician does not maintain the track because he has not been instructed to do so. As a result, the track is outside of tolerance which could lead to a derailment – linked to H1	No instruction			✓
Track section Mgr								
	Maintenance schedule							
		✓		Sen1: The maintenance schedule is not implemented due to and oversight. As a result, the track is outside of tolerance which could lead to a derailment – linked to H2	oversight			✓

Controller	Control actions	Scenario type		Scenarios	Causes	Source verification		
		Control action not implemented	Control action improperly implemented			Source incident facts	Source context facts	No facts found
	Instruct and enforce standards							
		✓		Sen1: The track section manager does not instruct the standards because he has received no instruction to do so. As a result, maintenance is carried out to inappropriate standards leading to a possible derailment – linked to H2	No instruction			✓
		✓		Sen2: the track section manager does not instruct the standards because he does not understand them. As a result, maintenance is carried out to inappropriate standards leading to a possible derailment – linked to H2	Lack of knowledge			✓
	Inspect track, decide if safe							
		✓		Sen1: The track is not inspected correctly and the track section manager is unable to decide if the track is safe – linked to H2	Not enough information			✓
	Report decision							
			✓	Sen1: The decision of whether the track is safe or not is not reported clearly leading to misinformation – linked to H2	Unclear reporting			✓
Area Controller								
	Ask information							

Controller	Control actions	Scenario type		Scenarios	Causes	Source verification		
		Control action not implemented	Control action improperly implemented			Source incident facts	Source context facts	No facts found
		✓		Sen1: The request for information is not given because it is not considered necessary – linked to H2	Misjudgement			✓
			✓	Sen2: The request for information is not conveyed properly and as a result it is not provided – linked to H2	Unclear communication	17		
	Instruct closure							
		✓		Sen1: The instruction to close the line is not given because it is not thought necessary	Misjudgement	16		
	Ask to investigate							
		✓		Sen1: The request to investigate is not given because it is not considered necessary – linked to H2	Misjudgement			✓
			✓	Sen2: The request to investigate is not conveyed properly and as a result it is not provided – linked to H2	Unclear communication	17		
Corporate Operations								
	Set/issue standards							
		✓		Sen1: Standards are not issued because they are not ready for publication. As a result, old standards are used in the field and incorrect limits are applied – linked to H2	Not available			✓
Corporate Engineering								

Controller	Control actions	Scenario type		Scenarios	Causes	Source verification		
		Control action not implemented	Control action improperly implemented			Source incident facts	Source context facts	No facts found
	Set/issue standards							
		✓		Sen1: Standards are not issued because they are not ready for publication. As a result, old standards are used in the field and incorrect limits are applied – linked to H1	Not available			✓
Driver								
	Control train							
			✓	Sen1: The driver does not control the train correctly and is unable to stop the train when required. – Linked to H3	Misjudgement			✓

Scenarios for controlled process without Unsafe Control Actions

Table 123 Scenario analysis for the controlled process

Controlled process component	Requirement	Scenario type			Scenarios	Causes	Source verification		
		Failure	Unplanned or no response	Delayed response			Source incident facts	Source context facts	No facts found
Drainage									
	Remove water from the track		✓		Sen1: Flood water overwhelms the drainage system leaving water flowing down the track. As a result, the track bed is washed away – linked to H1	Drainage overwhelmed	19		
		✓			Sen2: The drainage is blocked leaving water flowing down the track. As a result, the track bed is washed away – linked to H1	Drainage failure			✓
Track bed									
	Support the rails and weight of trains	✓			Sen1: The track bed does not resist the flow of water. As a result, the track is left unsupported – linked to H1	No resistance to water	21		
Track									
	Support the weight and provide a guide path for trains	✓			Sen1: The rails distort and do not provide a guide path for the trains. As a result, the train derailed – linked to H1	Rails move			✓
		✓			Sen2: The rails are unable to support the weight of the train and bend which causes a derailment – linked to H1	Rails move	21		

H3.5 Analysis interpretation

The analysis has described a large number of potential causes and scenarios.

Meaning can only be extracted through interpretation of the analysis tables in the context of the incident. This stage is not part of the STPA process.

It is noted that most of the results concentrate on the communication and control actions of those involved. The physical system is only analysed in the last table.

There is no explicit indication of the level of risk expressed by each section.

Source data verification has been appended to the scenario tables to indicate the statements that are supported by evidence from the field. These indications show that at least one fact statement in Appendix D supports the scenario statement. As can be seen there are a significant number of unsupported statements, 90 in total, while 28 are supported, 24%.

Appendix I - Baidon incident Yellow Book risk analysis

This analysis has been carried using methods from the Yellow Book (Rail Safety and Standards Board, 2007) as part of a case study to benchmark the CAM analysis method. The analysis has been carried out using the publicly available information, from an RAIB investigation report (Rail Accident Investigation Branch, 2017) which has been created from their analysis. The particulars of the incident are contained in Appendix D. The analysis method chosen is representative of an established way of carrying out system safety risk analysis in the rail industry. The outcome is used to compare and contrast with other methods of analysis including CAM.

The analysis has been simplified to enable a rapid development of the method, given the limited detail available, and therefore hazard identification has been limited in this case to the essential facts.

Appendix Contents

I1 Assessment of risk

487

I2 Method used

489

I3 Analysis	
I3.1 Hazard identification	489
I3.2 FMECA – causal analysis	489
I3.3 Summarised risk analysis	498
	503

I1 Assessment of risk

For the purposes of this analysis a semi-qualitative method of assessing risk has been used based on EN50126 (CENELEC, 2017), shown in Table 124, as a calibrated likelihood-consequence table. The frequency scaling has been performed assuming a system life span of 20 years, on the basis that process and operating practices are unlikely to remain unaltered beyond that point.

Table 124 Risk matrix formulated from (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic	
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable	<1yr
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable	<2yrs
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable	<5yrs
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable	<10yrs
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	<20yrs
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable	≥20yrs

I2 Method used

The method employed is set out in the industry Yellow Book publication (Rail Safety and Standards Board, 2007) as the 7 stage process. In this case not all the stages are required.

The analysis is set out below:

1. Hazard identification
2. Causal analysis or
3. Consequence analysis
4. Loss analysis
5. Options analysis
6. Impact analysis
7. Demonstration of acceptability

Stages 3 to 6 are not used. Stage 7 is partially used to provide a calibrated risk matrix.

I3 Analysis

The particulars of the Baildon incident are contained in Appendix D.

I3.1 Hazard identification

The boundary of the system is set as the railway system within the track section reported, including those responsible for maintaining and controlling it. The system

includes the section of the culvert directly under the railway, but not other parts of it. There is an interaction with drainage water and the environment generally. The interfaces are documented in Table 125

Table 125 Interface list

Interface	Comment
Beck culvert	Water is drained from one side of the railway into the river.
Connected railway	Trains appear and are removed from the system over the tracks to other locations.
Environment	The railway is exposed to the environment.
Public and other organisations	There is a communications interface to others.
Other part of the organisation	There is a communications interface to other parts of the organisation.

In this case the identification will be undertaken using an empirical method using an FMEA because the hazards are based on the report.

I3.1.1 FMEA - identification

The object of this stage of the process is to identify the hazards through a functional analysis. A desktop FMEA analysis has been conducted using EN60821 (CENELEC, 2006) and Anleitner (2010) and tailored to a safety application in a similar way to Mohr (2002). The approach has been to treat the systems as performing a function and then to document the failure of the function. A high detection number of 10 indicates that it will be easy to detect and prevent through the applied controls, conversely a low score indicates that the failure is difficult to detect and therefore may be latent. The classification is S for a significant function failure and C for a critical failure where there is a direct safety implication. Classification conversions, if necessary, from S to C are performed by adjusting the occurrence to reflect that not every failure will result in a safety event as articulated by Lepmets (2017). Also, consideration will be taken of the effect of detection and controls when setting the occurrence in the case of a safety classification. The RPN field is not considered appropriate for this particular application. These risk parameters will be assessed later in the analysis.

The source facts columns have been appended to provide traceability to the evidence contained in Appendix D and indicate that each FMEA entry is justifiable.

Table 126 FMEA for rail system

Ref	Item	Functional requirement	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
101	Culvert	Support the ground above	Failure during operation	Structural collapse	Land subsides			Too much weight on structure		Design codes	Reports from railway	5		The culvert will cease functioning	1	1
102	Culvert	Water volume flow	Failure during operation	Water leaks out of inspection manholes	water flows down embankment			Pressure too high		Control of pressure and flow volume	Reports from surrounding area and calculations	5		The pressure forces the water to rise up the inspection manholes and pop the covers	2	2, 3

Ref	Item	Functional requirement	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
103	Ballast	Support sleepers	Failure during operation	Washed away	Sleepers unsupported			Strong waterflow		Keep water in drains or fit retaining mesh to ballast. Also GE/RT8000 -M3 stopping trains	Inspection and reports	3		If the sleepers are left in mid-air a train will cause the rails to bend and possibly cause a train to overturn or derail	2, 5, 14	
104	Sleepers	Support load	Failure during operation	Sleeper not supported	Rails dip			No ballast		Retain ballast	Inspection and reports	3		If the sleepers are left in mid-air a train will cause the rails to bend and possibly cause a train to overturn or derail	5, 21, 23	
105	Train	Move off rails	Failure during operation	Derailment	Fatality			Rails fail to support train		Signalling	Inspection and reports	5		If the train derails there is a risk that there could be casualties	5, 10, 21	
106	Mtce Engineer	Spot faults	Failure during operation	Failure to spot fault	Derailment			Missed fault		Instructions Training	Subsequent inspections Reports by others	2			8, 17, 19	
107	MoM	Spot faults	Failure during operation	Failure to spot fault	Derailment			Missed fault		Instructions Local knowledge	Subsequent inspections Reports by others	2			4, 8, 17, 18	
108	MoM	Spot faults	Failure during operation	Failure to spot fault	Derailment			No access		Make sure MOM is able to access railway	Certification	2			3	

Ref	Item	Functional requirement	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment	Source incident facts	Source context facts
109	Signaller	Stop trains	Failure to operate at prescribed time	Not stop trains	Derailment			Incorrect decision		Training Supervision	Monitoring Driver reports	2			6	
110	Route controller	Receive an emergency message	Failure to operate at prescribed time	Not act on message	Derailment			Incorrect decision		Training Supervision	Monitoring	2			16	
111	Route controller	Instruct signaller	Failure during operation	Fail to give clear instruction	Derailment			Lapse		1 Registers 2 Safety critical Comms	Monitoring via voice recorder	2		There are examples of lapses but the consequence is averted by the driver or signaller	22	
112	Route controller	Receive emergency message	Failure during operation	Fail to interpret message correctly	Derailment			Limited local knowledge		1 Training	Monitoring via voice recorder	2			7	

Calibrating the hazard table from values given Appendix D of the Yellow Book (Rail Safety and Standards Board, 2007)

Table 127 Definition of risk components (Rail Safety and Standards Board, 2007)

Frequency category	Definition
1	Less than 100 yearly
2	10 to 100 years
3	1 to 10 years
4	Monthly to yearly
5	Daily to monthly
Severity category	Definition
1	Minor injury
2	Major injury
3	Multiple Major injuries
4	Single fatality
5	Multiple fatalities

Table 128 Hazard ranking matrix

Ref	Hazard description	Estimated frequency	Estimated severity	Hazard rank	Comments
101	Structural collapse	2	3	6	A structural collapse of the culvert under the railway would cause a problem but a train would have to be in the vicinity at the time

Ref	Hazard description	Estimated frequency	Estimated severity	Hazard rank	Comments
102	Water flows down embankment	4	1	4	Water flowing down the embankment will not in itself cause a problem if it is drained properly
103	Ballast washed away	3	4	12	If the track is not supported a train is likely to derail. It is likely that at least one train would come across the fault and thus have a risk of derailment
104	Rails dip	3	3	9	If the rails dip it is likely that the train will be unstable and could result in injuries
105	Derailment	3	4	12	If the train is derailed and rolls, from past performance there is likely to be a fatality. However, if it stays upright injuries are likely to be less severe. In this case there is a one sided embankment and there is a possibility of a roll.
106	Missed fault	4	2	4	Engineering inspection faults are missed and could lead to an injury. However, it is extremely rare that a single missed fault would lead directly to a serious accident, it is much more likely to lead to serious damage to equipment.
107	Missed fault	4	4	16	When a MOM is tasked with inspecting a fault, someone has reported it and considers it dangerous. As a result, it is

Ref	Hazard description	Estimated frequency	Estimated severity	Hazard rank	Comments
					more likely that it would lead to a serious outcome.
108	No access	3	2	6	A requirement of the MOM's job is to be certified for access to the track. If this limitation is known then procedures should make sure that an alternate undertakes the job. Therefore, the outcome is not likely to be serious, more a matter of inconvenience
109	Trains not stopped	3	4	12	There is a significant level of supervision of signallers that results in a low incidence of errors.
110	Delay in stopping trains	3	4	12	Communications are monitored although there was confusion between the controllers over the nature of the incident. It would be the norm for the area controller whose area the communications concerned to deal with the call.
111	Unclear stop instruction	3	4	12	There is a monitored communications protocol and therefore there is pressure to make sure that communication is clear.
112	Received message not interpreted correctly	3	4	12	There is a chance that the received message is not interpreted correctly because it could come from an

Ref	Hazard description	Estimated frequency	Estimated severity	Hazard rank	Comments
					untrained source (not using protocols). However, training is in place for this.

I3.2 FMECA – causal analysis

The Yellow Book (Rail Safety and Standards Board, 2007) identifies FMEA as a suitable process and points to EN50129 (CENELEC, 2003) which in turn points to EN60812 (CENELEC, 2006) for the FMEA and FMECA. The objective for this stage of the process is to analyse the hazards through a functional analysis. It is designed to provide two pieces of rating information the Risk Priority Numbers (RPN) and frequency and severity values that can be used in a risk matrix.

A desktop FMECA analysis has been conducted using EN60812 (CENELEC, 2006) and Anleitner (2010). The approach has been to treat the systems and people as performing a function and then to document the failure of the function. The classification has been taken as whether the function has catastrophically failed or has been severely affected. Likewise, the severity has been classified on the impact of the functional failure. A high detection number of 10 indicates that it will be easy to detect, conversely a low score indicates that the failure is difficult to detect and therefore may be latent.

The figures in Table 130 have been manipulated in a similar manner to that described in EN60812 section 5.3 (CENELEC, 2006) using severity and occurrence values derived from EN50126 (CENELEC, 2017). These are used to create an RPN value by multiplying them with the detection number subtracted from 10. This done to create RPNs that are lower for easily detected hazardous faults. The manipulated values of given in parentheses in red.

The severity and occurrence scores are taken and mapped onto a risk matrix.

Table 129 Scaling table for severity and occurrence formulated from (CENELEC, 2017)

Occurrence Category	Value	Definition
Frequent	6	Less than a year
Probable	5	Less than 2 years
Occasional	4	Less than 5 years
Rare	3	Less than 10 years
Improbable	2	Less than 20 years
Highly Improbable	1	Greater or equal to 20 years
Category	Value	Definition
Catastrophic	5	Multiple fatalities
Critical	4	Fatality/multiple major injuries
Major	3	Life changing injury
Marginal	2	Injury
Insignificant	1	No material harm

Table 130 FMECA for rail system

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
101	Culvert	Support the ground above	Failure during operation	Structural collapse	Land subsides	(4)	C	Too much weight on structure	20yr (2)	Design codes	Reports from railway	5 (5)	40	The culvert will cease functioning and could cause a derailment if the ground dropped as a result. However, the track is inspected every week and it is more likely that a rough ride would be experienced than a derailment, which would be reported and corrected

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
102	Culvert	Water volume flow	Failure during operation	Water leaks out of inspection manholes	water flows down embankment	(2)	S	Pressure too high	1yr (5)	Control of pressure and flow volume	Reports from surrounding area and calculations	5 (5)	50	The pressure forces the water to rise up the inspection manholes and pop the covers. The flow of water is not in itself a problem as long as it is drained from the railway correctly.
103	Ballast	Support sleepers	Failure during operation	Washed away	Sleepers unsupported	(4)	C	Strong waterflow	4yr 5yrs (3)	Keep water in drains or fit retaining mesh to ballast. Also, GE/RT8000 -M3 stopping trains	Inspection and reports	7 (3)	36	If the sleepers are left in mid-air a train will cause the rails to bend and possibly cause a train to overturn or derail. However, there is a standing instruction in the rule book to stop trains should flooding occur above rail height. The report refers to this. Therefore, for this to be a safety problem the water would not have been spotted or the rule book not applied. Even though the ballast could be washed away, from a safety perspective it is estimated that the frequency will be reduced to the order of 5yrs
104	Sleepers	Support load	Failure during operation	Sleeper not supported	Rails dip	(4)	C	No ballast	4yr 5yrs (3)	Retain ballast	Inspection and reports	4 (6)	72	If the sleepers are left in mid-air a train will cause the rails to bend and possibly cause a train to overturn or derail. However, there is a standing instruction in the rule book to stop trains should flooding occur above rail height. The report refers to this. Therefore, for this to be a safety problem the water would not have been spotted or the rule book not applied. Even though the ballast could be washed away, from a safety perspective it is estimated that the frequency will be reduced to the order of 5yrs
105	Train	Move off rails	Failure during operation	Derailment	Fatality	(4)	C	Rails fail to support train	10yrs (2)	Signalling	Inspection and reports	5 (5)	40	If the train derails there is a risk that there could be casualties. However, it is influenced by whether the train remains upright.

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
106	Mtce Engineer	Spot faults	Failure during operation	Failure to spot fault	Derailment	(3)	C	Missed fault	3m 5yrs (3)	Instructions Training	Subsequent inspections Reports by others	2 (8)	72	There is a likelihood of things being missed in a human inspection. However, there are margins built into designs that allow for a missed item. As long as a fault is spotted before it becomes dangerous the inspection failure is not significant. Therefore, the significant frequency is judged not to be 3 months by 5 years
107	MoM	Spot faults	Failure during operation	Failure to spot fault	Derailment	(3)	C	Missed fault	4yr 3m (6)	Instructions Local knowledge	Subsequent inspections Reports by others	2 (8)	144	The frequency of the event is low (an on-demand emergency situation). Given that a critical failure is reported then the consequences of missing a fault are more likely to occur
108	MoM	Spot faults	Failure during operation	Failure to spot fault	Derailment	(4)	C	No access	10Yrs (2)	Make sure MOM is able to access railway	Certification	8 (2)	16	The lack of certification is highly likely to be known to management. The norm is for cover to be arranged by someone who is certified. Any lapse is likely to be spotted through management procedures.
109	Signaller	Stop trains	Failure to operate at prescribed time	Not stop trains	Derailment	(4)	C	Incorrect decision	10yrs (2)	Training Supervision	Monitoring Driver reports	2 (8)	64	Signallers are heavily supervised and their actions are recorded. It is unlikely that trains would be routed incorrectly given the training and supervision and that the action would not be spotted and corrected.
110	Route controller	Receive an emergency message	Failure to operate at prescribed time	Not act on message	Derailment	(4)	C	Incorrect decision	5yrs (3)	Training Supervision	Monitoring	2 (8)	96	This was primarily caused by a difference in understanding between the 3 route controllers about the nature of the incident. Route controllers are given training is to prevent omissions and errors.
111	Route controller	Instruct signaller	Failure during operation	Fail to give clear instruction	Derailment	(4)	C	Lapse	10yr 5yrs (3)	1 Registers 2 Safety critical Comms	Monitoring via voice recorder	2 (8)	96	There are examples of lapses but the consequence is averted by the driver or signaller in some cases. However, if the controller forgets there is little real-time supervision to correct the error. Therefore, the frequency is likely to be higher

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
112	Route controller	Receive emergency message	Failure during operation	Fail to interpret message correctly	Derailment	(4)	C	Limited local knowledge	5yrs (3)	1 Training	Monitoring via voice recorder	2 (8)	96	The knowledge of the local area is a skill and is assisted by the naming of structures. However, where there are lapses in recall or gaps in the moment there is little oversight.

13.3 Summarised risk analysis

The identified hazards are ranked using the matrix.

Table 131 Baildon risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent		102	107		
Probable					
Occasional			106	103, 104	
Rare				110, 111, 112	
Improbable				105, 108, 109	
Highly Improbable				101	

The unacceptable hazards indicated by the matrix are 102 and 107. In comparison 107 has a score of 144 the highest while 102 has a ranking to 50 which is lower than those associated with the signaller (110) and controller (111 and 112) which are at 96. While the hazard of no ballast under the sleeper (104) has an RPN of 72, but is considered tolerable.

Appendix J - CAM user instructions

Appendix Contents

J1 Introduction	504
J1.1 - Risk acceptance	508
J2 - CAM_FN for new/novel/modified designs	510
J3 CAM_FA for accident analysis	530
J4 CAM_RA for accident analysis	532

J1 Introduction

This Appendix provides a set of user instructions for the application of the Composite Assessment Method (CAM). The three variants of CAM are shown in Figure 56, two of the variants are optimised for accident analysis and the third is

primarily to be applied to new/novel or altered designs. Each variant has been given a shorthand label, which is indicated in Table 132.

Table 132 List of CAM variants

Method	Figure 56 diagram colour	Shorthand name
Forward New/novel/modified system method	Green	CAM_FN
Forward accident method	Orange	CAM_FA
Reverse accident method	Turquoise	CAM_RA

The CAM_FN variant is the core method and consists of five stages, with an iteration loop. This assumes that the safety risks are to be discovered through the analysis. The second variant CAM_FA takes the CAM_FN and adds a process at the beginning and the end to match the output to what happened in an accident. The third variant CAM_RA uses the process in reverse to discover the cause of an accident. In this case not all of the stages of a full CAM analysis are required.

Primarily these user instructions are organised around each variant of CAM. Each of the three variants are explained as full processes in separate subsections defined in the contents beginning with CAM_FN.

However, for practical purposes it may be more convenient to look at the instructions for a particular stage. Figure 56 contains boxed stage labels. It can be seen from the figure that the variants share stages. Each Stage is explained in a separate section as shown by the index in Table 133.

Table 133 Stage-page number index

Stage	1	2	3	4	5	A1	A2	B1	B2	B3	B4	B5	iteration
Page	512	513	518	524	528	532	532	535	535	535	536	539	528

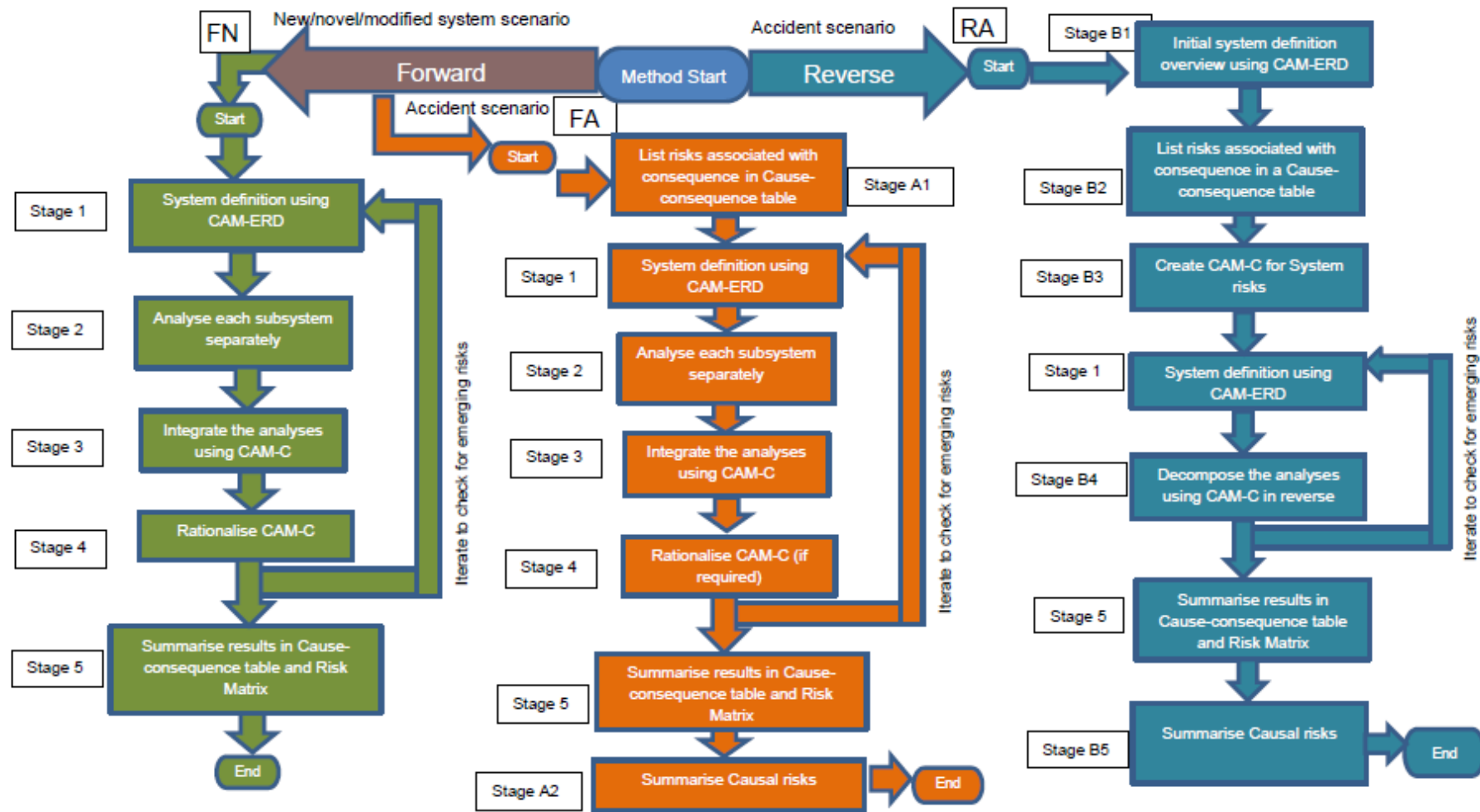


Figure 56 The three variants of CAM

J1.1 - Risk acceptance

One of the objectives of CAM is to meet the legal requirements of risk acceptability and to that end the scales used by the Author have been based around the risk matrix in EN50126 (CENELEC, 2017)

Table 134 Risk matrix (CENELEC, 2017)

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent	Tolerable	Intolerable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Tolerable	Intolerable	Intolerable	Intolerable
Occasional	Tolerable	Tolerable	Tolerable	Tolerable	Intolerable
Rare	Negligible	Negligible	Tolerable	Tolerable	Tolerable
Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable
Highly Improbable	Negligible	Negligible	Negligible	Tolerable	Tolerable

Green areas of the matrix are deemed 'broadly acceptable', yellow areas are 'tolerable' and the red areas are 'intolerable'. The rows represent the likelihood and the columns the consequence or severity of a risk. It is for the analyst to calibrate the matrix

likelihood to a timeframe, and the meaning of the consequence. There tends to be wide agreement on the meaning of the consequence, starting with Critical denoted as a fatality, and Major as a life changing injury and so on. There are industry publications that give further guidance such as 'Yellow Book' (Rail Safety and Standards Board, 2007), and guidance 'R2P2' from the HSE on risk acceptability (Health and Safety Executive, 2001) and ORR (Office of Rail and Road, 2018).

As a result, the Author has adopted 6-point likelihood (frequency) scale and 5-point consequence scale for qualitative assessments. These considerations influence some of the instructions for CAM.

J2 - CAM_FN for new/novel/modified designs

This variant is primarily designed to be used with new/novel/modified designs; however, it can be used for accident analysis if required although the other variants may be a more efficient option. A flow diagram of the process is shown in Figure 57.

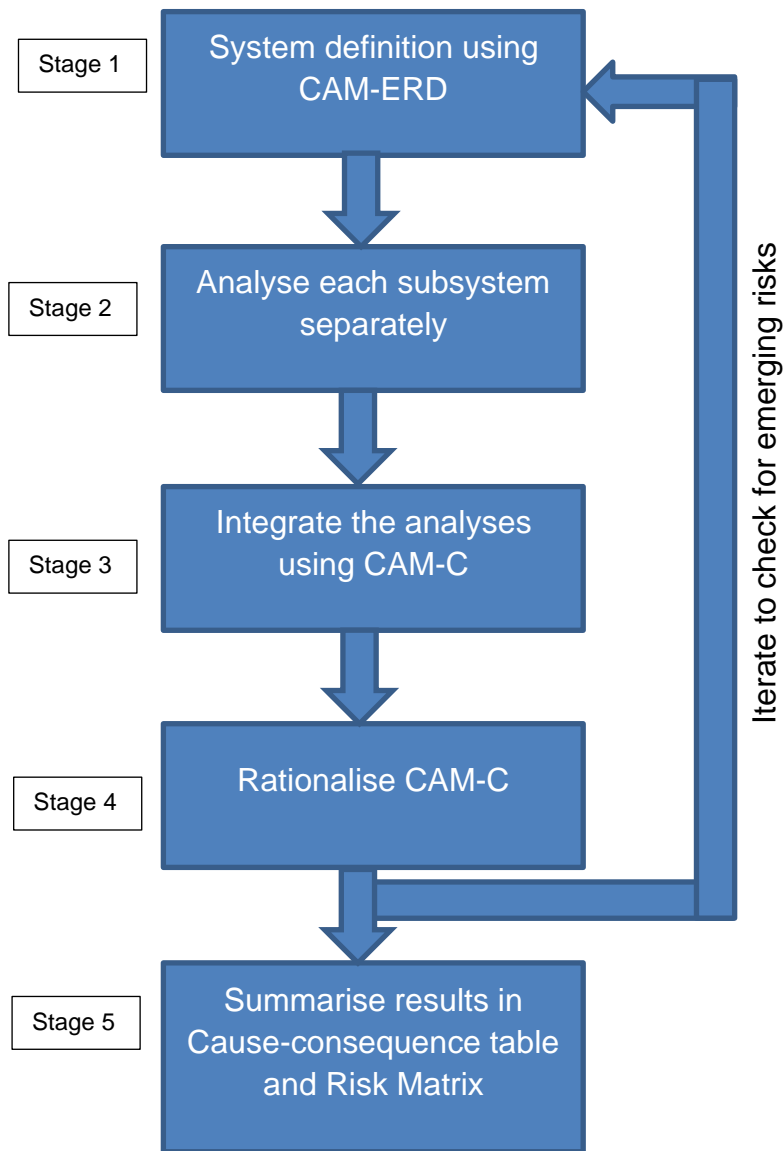


Figure 57 CAM_FN variant process

As can be seen there are five stages which build to a result plus an iteration process. As an introduction these can be summed up as first break the system to be examined down into parts for examination. Second examine these parts, third recombine and integrate these separate analyses into a single view. Forth rationalise the single view if necessary, to understand the result. Fifth, summarise the risks from the single view and present them in a form that is consistent with legal requirements and in a form to convey the information to non-analysts.

Finally, there is an iteration loop included in the method to repeat the analysis process to include any emerging risks as a result of the integration step of the analysis.

All of these stages are explained in more detail below

Stage 1 – system definition

To examine a system a limit on the analysis is required in the shape of a system boundary. Also, subsystems must to be defined together with their parts. This is done using CAM-ERD, which is a type of relationship diagram. The circles represent subsystems, rectangles represent parts and a red triangle represents a point of harm. These are connected by arrows that represent relationships. These relationships normally represent hazards/risks but other labels can be used to help understand the operation of the system in terms of risk. An example is shown in Figure 58. The CAM-ERD diagrams are constructed from documentation on the system. Brainstorming or HazOp techniques can be used as an aid to identify the hazards/risks and parts of the system.

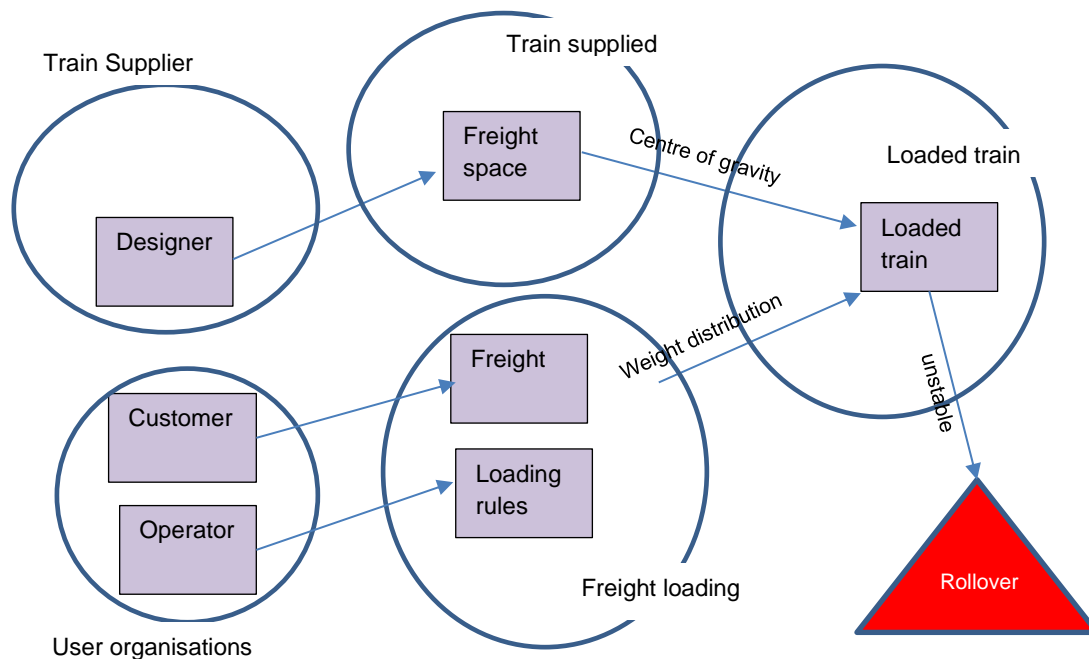


Figure 58 CAM-ERD example


To create a CAM-ERD:

1. decide what is to be included and excluded from the system to be analysed
2. identify and draw circles for the subsystems and label them
3. populate the subsystems with the relevant parts that represent functions within each subsystem and label them
4. identify the point or points of harm and place them near the appropriate subsystems. Label these points of harm.
5. draw and label arrows to identify the relationships between the parts, subsystems or both. Additionally, draw arrows to identify the direct relationships between the subsystems/parts and the point of harm

Stage 2 – subsystem analysis

For each subsystem identified in stage 1 carry out a risk assessment analysis using a technique of choice. Each of these subsystems is to be examined in isolation. Some of the techniques are easier to use with CAM than others Table 135 gives an indication.

Table 135 Ease of use recommendation



Technique	Comment
Cause-consequence	A tabulated form that fits with the CAM-C matrix and directly lists risks
FMEA	A tabulated form that fits with the CAM-C matrix. Ideally, failures need to be re-expressed in risk form in CAM-C
FMECA	A tabulated form that fits with a matrix. Ideally, failures need to be re-expressed in risk form in CAM-C
FTA	Pictorial view of the risk of a top event. Could require many FTAs to cover the scope. Each FTA maps only one top level event.
Reliability Block diagram	Pictorial view of the risk of a top event. Could require many RBD to cover the scope
Bow Tie	As per FTA and ETA as long as it is derived from them. Otherwise needs to be translated into a risk form and evaluated
Accimap	Data needs to be translated into a table.
SCM	Once events are identified the values can be used as part of the CAM-C
FRAM	The values from the model can be taken and used in the CAM-C
Bayesian Networks	The JPL values can be used in the CAM-C
ETA	Pictorial view of event outcomes. Could require many ETA to cover the scope and suitable for post-event consequence analysis only. The causal information is missing and would have to be supplemented through another technique.

These techniques are explained in other publications. However, by way of an example, an extract for an FMEA is included, Table 137. The meaning of the

columns for this interpretation of FMEA²⁰ is shown in Table 136 with information from (Anleitner, 2010) and EN60812 (CENELEC, 2006).

Table 136 Modified FMEA column description (Anleitner, 2010) and EN60812 (CENELEC, 2006)

Column	Description
Ref	Reference number for row.
Item	Subsystem part.
Functional requirements	The function that the part is required to fulfil (for safety).
Potential failure type	The type of failure design/operation.
Potential failure mode	Failure description of how the subsystem could fail.
Potential failure effects	The effect of the failure on the subsystem and overall system (where appropriate).
Severity	An enumerated value. The Author uses 1-5 and linked to EN50126 levels, as explained earlier.
Classification	C=Critical, where there is a safety failure. S= Significant, where there is a major functional failure.
Potential cause or mechanism	The cause of the failure
Occurrence	The likely frequency of the failure
Controls for prevention	Controls that are in place to prevent the failure.
Controls for detection	Controls that are in place to detect the failure before it occurs.
Detection	An enumerated number 1-10, where 10 means that it is highly likely to be detected.
RPN	Not used.
Comment	Other relevant information.

²⁰ There are slight differences in interpretation of the various columns from various writers, although the core meaning is consistent. For example, some writers would call this interpretation a FMECA.

Table 137 FMEA sample extract

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
101	Path	Solid foot way	Failure during operation	Path breaks up	Uneven surface And exposed meters Tripping likely	2	S	Water drainage	1m	Choice of material	Inspection and surveys	8		If the path is washed away the buried service equipment may be exposed. Furthermore, it will be difficult to function as a walkway.

Ref	Item	Functional requirements	Potential failure type	Potential failure mode	Potential failure effects	Severity	Classification	Potential cause or mechanism of failure	Occurrence	Controls for prevention	Controls for detection	Detection	RPN	Comment
104	Material	Stable even surface	Failure during operation	Material washed away	Uneven surface And exposed meters Tripping likely	4	S	Water flow downhill causing scouring	1m	Choice of material packing and containment	Inspection and surveys	5		This is water volume/flow and materials dependent. However, current performance shows that the path material is susceptible to water flow.

Stage 3 – integrate the analysis

This stage is the most complex to explain because of the number of associated concepts, but it is simple to apply in practice.

The analyses undertaken in stage 2 are integrated into a single view in this stage using a CAM-C. It is used for several purposes, first to combine the analyses, second to rationalise the output, third to trace risks to root causes; these are explained in the following sections, with rationalisation deferred to stage 4.

Conceptually subsystems can be connected together through the interfaces at their boundaries; these interconnections are links. Subsystems that have no interfaces are isolated within a system and have no tangible effect. In this way it is possible for risks to pass between subsystems and have an effect on the overall system and the world beyond. CAM-C in concept represents links between subsystems that are capable of transmitting risks from one subsystem to another. The transmission could cause the severity of the risk to be modified.

CAM-C is a matrix which is similar to a spreadsheet. The columns represent the causal risks and the rows represent the output risks.

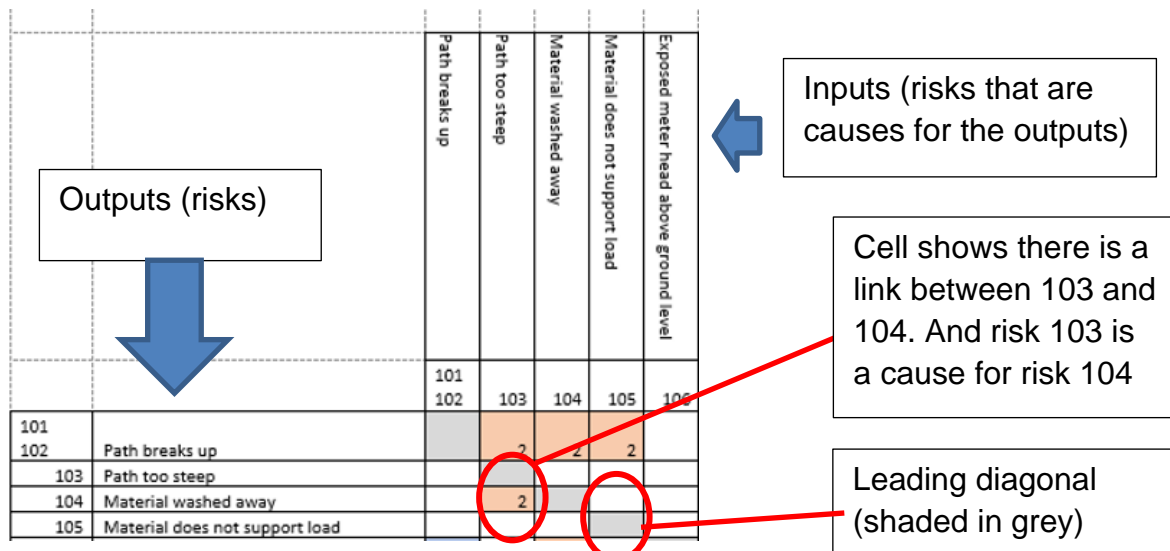


Figure 59 An illustrative example extracted from a CAM-C

An example CAM-C is shown in Figure 59, the risks are labelled together with reference numbers, so reference 103 represents the risk 'Path too steep'. As can be seen a link between subsystems is denoted by the presence of a figure in an intersecting cell, in this example 103 is a causal risk for 104.

As was stated a figure in an intersecting cell indicates that a link exists. A link is formed based on the belief that there is a risk influence from one subsystem on another; this could be due to energy transfer, a mechanical linkage or information flow between the subsystems. If it is believed there is no influence then the cell is left blank. The type of link could be an amplification of the risk from one subsystem to another, or a reduction in the level of risk in the following subsystem, or a continuation of the risk at the same level in the following subsystem. These three types of link are known as amplifier, resistor and carrier respectively. There is a further type of link where the resistive property is high enough to effectively stop the risk, this is known as a terminator.

It is possible for CAM to be used to model either a qualitative or quantitative analysis. If a quantitative analysis is undertaken the figures in the cells will reflect

the actual value of the risks. However, in the case of a qualitative model the figures in the cells are enumerators; the suggested values are shown in Table 138.

Table 138 CAM-C values

	Mode	
	Qualitative	Quantitative
Link-type	Cell enumerator	Cell scalar
No link	Blank	Blank
Amplifier	3	$x > 1$
Carrier	2	$x = 1$
Resistor	1	$0 > x < 1$
Terminator	-10	$x = 0$

Where x is the cell scalar value.

So, in Figure 59 the link between 103 and 104 represents a carrier type for a qualitative model or a small amplifier in a quantitative model.

An example CAM-C is shown in Figure 60, it consists of three subsystems these are given reference number ranges 100-199, 200-299, and 300-399 respectively. As can be seen the individual subsystem risks are grouped by subsystem. A column and row entry are created for each risk. Link numbers are inserted where it is believed there is a connection.

CAM-C assumes for each row that the individual causal risks are related to the output risk by a logical OR relationship; where each causal risk contributes a portion of the total output risk. Furthermore, using an iterative link from column to a row, implies a logical AND relationship in a chain, albeit a simplified one. However, some risks only materialise when several causes on that row occur at the same time. The individual causal risks are in this case related through a logical

AND relationship. CAM also provides for this type of AND relationship in the model. The analyst inserts a special row to indicate that it must be handled slightly differently in the assessment. The effect is to reduce the likelihood of the risk's occurrence by assigning the lowest frequency of the causal risks to the output. This type of row is denoted by 'AND' label on the leading diagonal. Figure 60 gives an illustration of the AND relationship for risk 304, it is dependent on the causal risks 201 and 202/203; both have to occur for risk 304 to be realised.

		Path breaks up	Material washed away	Material does not support load	Exposed meter head above ground level	Structural failure	No friction	Loss of grip	Fall off	Fail to stop	Bike skids away	Mechanical failure
		101	104	105	106	201	202 203	204	301	302	303	304
101	Path breaks up		2	2								
104	Material washed away											
105	Material does not support load											
106	Exposed meter head above ground level	3	3									
201	Structural failure											
202 203	No friction											
204 206	Loss of grip											
301	Fall off	2	2	2	3	-10		2			2	2
302	Fail to stop									PD	2	
303	Bike skids away											
304	Mechanical failure					2	2					AND

Figure 60 Illustrative CAM-C example

The power of the CAM-C comes from the ability to trace risks through the matrix between subsystems. This is explained by-way of another illustration.

			Culvert			Pipes	Ballast		Sleepers		Drain
			101 102	103	104	105	201	202	203	204	205
Culvert											
	101 102	Blocked									
	103	Structural collapse									
	104	Water leaks out of manholes			3						
Pipes											
	105	Flow not enough									
Ballast											
	201	Fallen away									
	202	Washed away									1
Sleepers											
	203	Moved		2							
	204	Sleeper not supported					3	3		AND	
Drainage											
	205	Overwhelmed			2						

Figure 61 Multi-subsystem CAM-C tracing illustration example

To trace a risk from an output to a root cause the analyst carries out an iterative process as follows. The analyst looks along the row of an overall-system risk and identifies the inputs; this is where a figure corresponds to a column. In this case 205 has a “2” in risk 104 column. The column is a risk, which is a causal risk contributing to the higher-level risk. This causal risk is then used as the next risk row to be traced. In this case risk 104. The process identifies causal risk iteratively until the path (trace sequence) terminates. In this case 105, the pipe risk of ‘flow not enough’ is the root causal risk.

To create a CAM-C for a qualitative model

1. extract the risks from the stage 2 analyses and group them into subsystems. Assign each risk a reference number
2. Use a large matrix (possibly in a spreadsheet application) and enter each risk as a heading for the rows and columns forming a square matrix.
3. grey out the cells on the leading diagonal
4. Where it is believed there is an interface which can transmit risk between or within subsystems enter a number according to Table 138 to represent the type of link.
5. Where the output risk is believed only to be partially described by the causal risks on the row insert 'PD' on the leading diagonal. (explained in stage 4)
6. Where the output risk relationship to the causal risks is believed to be of an AND type insert a 'AND' on the leading diagonal.

Stage 4 – rationalisation

The CAM-C now contains a matrix of the risks, and in a complex system the relationships could be complicated which will make it difficult to understand which are the critical risks. Rationalisation is a process to ease this problem, it involves eliminating some risks from the analysis by altering the CAM-C. The methods are:

- Remove intermediate risks
- Remove internal risks
- Remove risks that rely on terminator links
- Remove duplicate risks
- Limit the analysis detail to a level that is useful

The main concept of rationalisation is that if the all the risks on a row completely explain and account for the output risk then the output risk can be substituted by these causal risks. If this process is repeated iteratively eventually a point will be

reached where it is no longer possible to substitute, these remaining causal risks are the root causes, which completely describe the system risks from a root cause perspective.

CAM-C can be used to remove intermediate and system-level risks from the analysis and identify the root causes through the trace. This action is logically valid only when the aggregate of the causal risks on the row describes the risk entirely. Where this is not the case that risk row must be retained, because there is some unique quality extra to the causes and the risk is designated as 'partially described'. This property is signified in CAM-C by placing a partially described (PD) label on the leading diagonal, an example is shown in Figure 60 for risk 302. In this case, 302 relies on skidding as described by 303, but there is also an element of misjudgement which is unique to 302, hence it is retained in the analysis.

The same restriction applies to the AND row where it is not possible to dissect the risk because all the causal risks have to occur at the same time. Therefore, the risk must be retained in the analysis.

Further rationalisation is possible through three mechanisms. These are based on two premises: for a subsystem risk to affect the overall system, it must interface to it. Furthermore, the subsystem risk has to be able to transmit the risk through intervening subsystems to the overall system. The first rationalisation mechanism is to eliminate those risks that only feed causes within a single subsystem because they will not influence the overall system. Second, is to eliminate those causal risks that link to a risk by terminator links because these are prevented from influencing the overall system. Third, eliminate any duplicate causal risks

because they have already been accounted for in the risk analysis. These eliminated elements do not need to be considered further in the analysis. An example is given in Figure 62.

		Path breaks up	Path too steep	Material washed away	Material does not support load	Exposed meter head above ground level	Structural failure	No friction	Loss of grip	Loss of grip and bike skids away	Fall off	Fall to stop
		101 102	103	104	105	106	201	202 203	204 206	205	301	302
101	Path breaks up		2	2	2							
102	Path breaks up											
103	Path too steep			2								
104	Material washed away											
105	Material does not support load											
106	Exposed meter head above ground level	3		3								
201	Structural failure											
202	No friction											
203	No friction											
204	Loss of grip											
206	Loss of grip											
205	Loss of grip and bike skids away											
301	Fall off	2		2	2	3	-10		2			
302	Fall to stop											PD

Figure 62 CAM-C example extract

The links coloured in orange all link within a single subsystem and therefore are not exported to any other subsystems. Removing the numbers from the matrix eliminates the links. Causal risk 201 is linked to risk 301 through a terminator link. This risk link can be similarly removed from the matrix. Removing the numbers from the CAM-C cells²¹ effectively eliminates the causal risks links from further consideration in the analysis.

The root cause tracing described above finds the root causes. Sometimes it might not be useful to identify these rather to terminate the trace at a point within the system instead. This curtailed trace and statement of risks is a matter for the analyst to decide and CAM facilitates it through the CAM-C mechanism.

To rationalise:

²¹ In practice it is better to colour code the cells just in case mistakes have been made during rationalisation.

1. colour those cell entries where risks link internally within a subsystem orange to indicate they should be removed from further consideration in the analysis.
 - a. Note: Internal linkages enable the analyst to understand how risks propagate through a subsystem, especially where it is complex. Under these circumstances it may not be clear at first sight that an input risk is related to another input risk with an output. Where there is a serial linkage between an input and output through a series of internal links care must be taken to ensure this input-output relationship is not lost in the rationalisation. The analyst should perform a mini rationalisation for the subsystem to relate the inputs to outputs and amend the CAM-C accordingly by making an entry to show the effect on the output subsystem of the input risk.
2. colour those cell entries where there is a terminator link in yellow to indicate they should be removed from further consideration in the analysis
3. colour one set of those cell entries light green where there are causal risks that are duplicates risks i.e., they describe the same risk in the output risk. This can occur where there are parallel paths for risks in the CAM-ERD and usually signifies double counting of the risk in the risk identification process. The coloured links can be removed from further consideration because the unmarked set describes the risk contribution.
4. colour cell entries for those causal risks and can be considered as summary risks for others within the same subsystem. In the example in

Figure 61, risk 101/102 is entitled 'path break up' which summarises risks like 104 'material washed away'. Later in the assessment they will indicate where options as to the depth of the analysis can be made. For, example ignore 101/102 and use 103, 104, and 105 instead or do the reverse and use 101/102.

5. At this point the removal of the intermediate links can be considered. Apply the trace process from the system level risks as described previously to identify the root causal risks. Mark each of these on the CAM-C. Note how many amplifier links have been traversed in each case. Note how many resistor links have been traversed on each case. Deduct the number of resistor links from the amplifier links and make a note of the resulting figure. This is best done on the output table in Stage 5 by adding additional columns to the right to hold the resulting figure for each case.

Iteration loop

The analysis and stages 1 through 4 should be reviewed to check for the effect of emergent risks that are observable in the overall system as a result of the integration process. Any risks that were not apparent at the subsystem level should be inserted into the analysis and checked to see if there is a material effect on the output of the analysis.

Stage 5 – summarise the output

The objective of this stage is to summarise the output in a form that is consistent with the legal requirements. A cause-consequence table as shown in Table 139 will meet the requirements.

Table 139 Cause-consequence table extract example

Ref	Title	Hazard	Cause	Description	Consequence scenario	Consequence description	Consequence	Control	Evaluation type	Likelihood	Consequence	Risk
104	Manhole leak	High Water flow	Pipes	Pipes do not allow enough flow causing pressure rise and water to burst out of manhole covers and flows at a high rate	Water flows onto the railway	Railway track bed is flooded, and water is fast flowing washing out ballast causing a derailment as injuries	Injuries and possible fatalities	Design control of flow and pressure	Risk Estimation	Occasional	Catastrophic	Intolerable
202	Ballast removal	Track unstable	Ballast washed away	The ballast is not fixed and is washed away by a flow of water	The track is unsupported and becomes unstable. It is unable to support a train	Track moves and derails a train causing injuries	Injuries and possible fatalities	Track inspection	Risk Estimation	Rare	Catastrophic	Tolerable

This is constructed by using the risks identified in the CAM-C and creating a row for each one which is derived from the subsystem analysis entry. In the case of an FMEA the columns are populated as indicated in Table 140.

Table 140 An Interpretation of the Cause-consequence table columns

Column	Description
Ref	Reference number of the risk
Title	A descriptive title composed from the FMEA row
Hazard	The state that could cause an adverse outcome
Cause	The state or action that caused the hazard to exist.
Description	A description of how the hazard could arise. Information from the potential cause or failure mechanism column can be used
Consequence scenario	This is a description of the possible outcome in terms of a sequence of events that could lead to an outcome
Consequence	A statement of the consequence in words.
Control	An action or state that acts to reduce or prevent a risk being realised.
Type of evaluation	In this case it will always be a risk estimation.
Likelihood	This uses an enumerated representation from the risk matrix of EN50126 as described earlier.
Consequence	This uses the value from the consequence column described above and converted using the EN50126 risk matrix as described earlier.
Risk	This uses a value from the EN50126 risk matrix described earlier obtained by looking up the likelihood and consequence values

The values in the last three columns are adjusted using the values noted in Stage four for the amplifier, resistor sums. Where there is a count of greater than zero

the likelihood should be increased by the number of categories indicated. Where there is a negative count, the likelihood should be reduced by the number of categories indicated. The cause-consequence table should now be adjusted for the root causes to reflect their impact at the system level.

Finally, the risks shown in the cause consequence table should be translated onto a risk matrix of the type described for EN50126. An illustrative example is shown in Table 141.

Table 141 Analysis summary risk matrix

	Insignificant	Marginal	Major	Critical	Catastrophic
Frequent					
Probable			R3		
Occasional		R1, R2, R5, R7			
Rare		R4			
Improbable					
Highly Improbable			R6		

J3 CAM_FA for accident analysis

This variant is designed to analyse accidents. The concept is to carry out an analysis in the same way as for the CAM_FN process, in effect an analysis from first principles. The output should among other risks contain the cause of the accident, this is extracted from the analysis and the root causes summarised. The analysis uses two additional processes to achieve this objective as highlighted in orange in Figure 63.

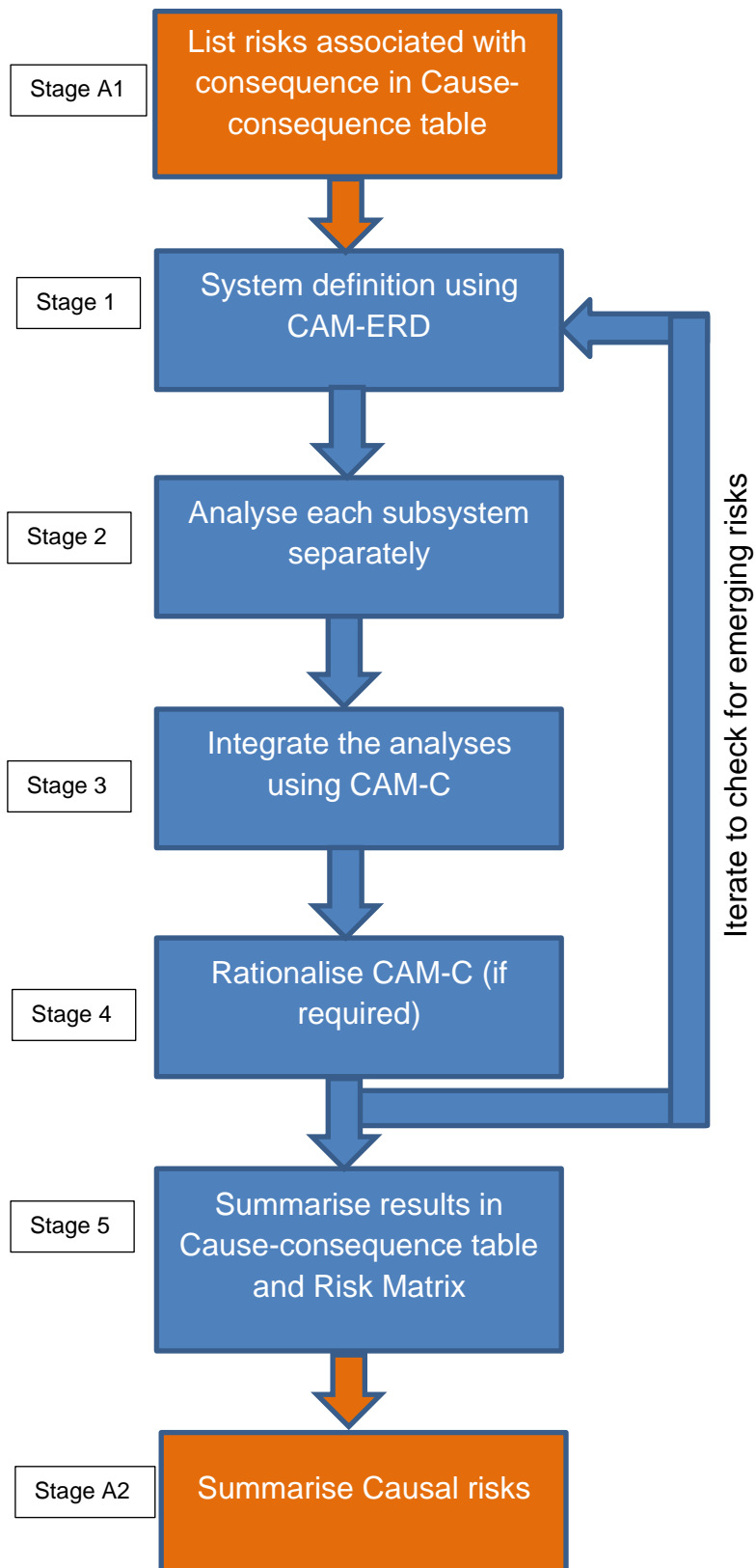


Figure 63 CAM adapted for post-accident analysis in the forward direction

As can be seen from Figure 63, stages 1 to 5 are the same as CAM-FN and the details are described in the CAM_FN section above.

Stage A1 – list risks

The objective is to use the information from the accident to frame a set of consequences using a cause-consequence table as shown in Table 139, and then fill in the rest of each row using information from the accident. The table may not be complete; however, the objective is to provide a target even if it is partial to use to filter the output of the analysis.

Stage A2 – summarise causal risks

Using the cause-consequence table from stage A1 filter the output of the analysis. Those risks that are indicated as relevant should be traced back to a cause in the output cause-consequence table from stage 5.

J4 CAM_RA for accident analysis

This variant is designed to analyse accidents, it avoids having to carry out a full analysis by operating CAM in reverse. As a result, not all the CAM process stages are required. A flow diagram for the variant is shown in Figure 64, as can be seen there are five new process, coloured green.

In concept this first uses the outcome of the accident to create a cause-consequence table of the consequences and causes at the top level. Second it uses this to create an initial CAM-C matrix to prime the process. Once this is done further versions of the CAM-C are generated to expand on the risks within the system and its subsystems. This process continues until a level is reached where

the analyst decides that the causes have been identified. The output is then summarised.

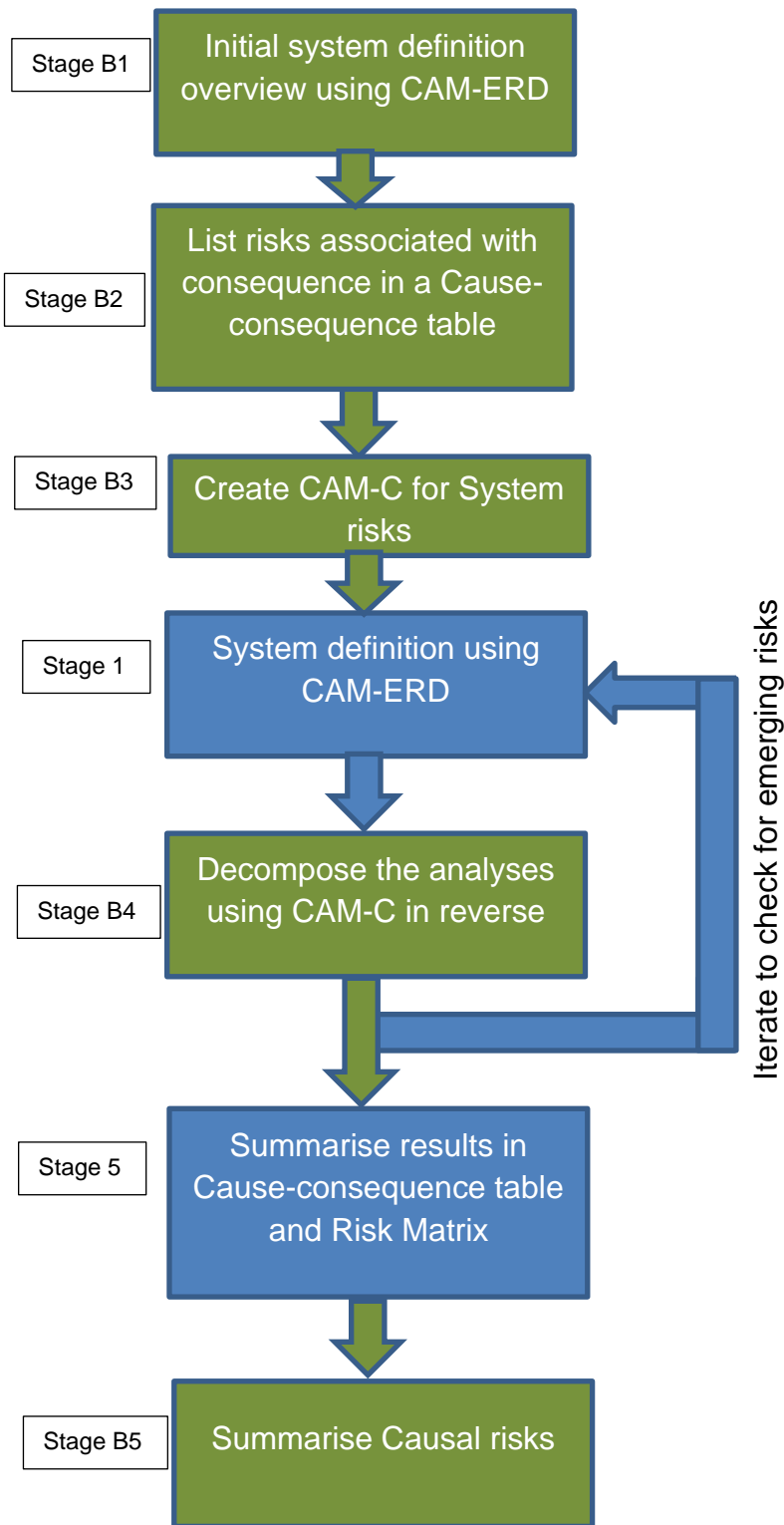


Figure 64 CAM adopted for accident analysis in the reverse direction

Stage B1 – create initial CAM-ERD overview

The objective is to create a CAM-ERD from the information gleaned from incident information to identify the main subsystems, parts and relationships at the system level to create an overview of the system being examined. At this stage some of the details and relationships may be missing but there should be enough information to create the lists required for Stage B2. The process used to create the CAM-ERD is the same as that described in Stage 1, however the information available may be incomplete at this stage of the analysis.

Stage B2 – list risks

The objective is to use the information from the accident to frame a set of consequences using a cause-consequence table as shown in Table 139, and then fill in the rest of each row using information from the accident. The table may not be complete; however, the objective is to provide enough information to form an initial CAM-C in the next stage.

Stage B3 – create CAM-C for risks

This stage uses a special form of CAM-C; the rows represent the top-level hazards and the columns the consequences. This provides a mapping from consequence to hazard. An example is shown in Table 142.

Use the list of risk from Stage B2 to create a CAM-C with the consequences as the row entries and the risks as the column entries. The cells linking the risks and consequences are to be filled in, mapping the consequences to risks. The entries in this case are a simple “yes” where a link exists.

A further column should be inserted in the CAM-C headed “evidence”. Where there is evidence to support the link a “yes” should be inserted in the cell.

Table 142 Reproduced illustrative CAM-C system level hazards – consequences

			Consequence property			
			Evidence	train out of control	MA incorrect	lineside error
Hazards	101	Trains off track	No			Yes
	102	Switch setting wrong	No			Yes
	103	Train speeding	No	Yes		
	104	Train speeding leaves track	No	Yes		
	105	Train outside MA	No	Yes		
	106	Faulty MA issued	Yes		Yes	
	107	Zone controller faulty start up	Yes		Yes	
	108	No train detected	No			Yes

Stage B4 – decompose the risks using CAM-C in reverse

This is created by using the trace method explained in Stage 3 of the CAM_FN process. However, in this case the column entries are generated by the analyst using information from the CAM-ERD and accident information to answer the question ‘What would cause this output risk?’. Table 143 shows an illustrative example.

Table 143 CAM-C for Zone controller - system level hazards

			System level hazards								
			Evidence	Trains off track	Switch setting wrong	Train speeding	Train speeding leaves track	Train outside MA	Faulty MA issued	Zone controller faulty start up	No train detected
				101	102	103	104	105	106	107	108
Controller Hazards	201	Controllers differ	Yes						3	3	
	202	New software unproven	Yes						2	3	
	203	Varying critical new functionality	Yes							3	
	204	System untestable	No						3	3	
	205	Live system has unproven data	No						2		
	206	System does not meet integrity level	Yes						3	3	

The cause-consequence table should be updated to reflect the uncovered risks and remove those that are of no interest i.e. where there is no evidence.

The process is continued via the iteration loop until the analyst has decided that enough information has been generated for the root causes to be attributed.

Stage B5 – summarise the causal risks

Extract the causal risks from the analysis and summarise them as the explanation of 'why' the accident has occurred. These are obtained from the CAM-C by identifying the causal risks from the columns that are linked to the risks listed in Stage B2. These are to be listed in the cause-consequence table first created in Stage 5.